

Polynomial invariants for a semisimple and cosemisimple Hopf algebra of finite dimension

Dedicated to Professor Noriaki Kawanaka on the occasion of his 60th birthday

Michihisa Wakui *

Department of Mathematics, Faculty of Engineering Science, Kansai University,
Suita-shi, Osaka 564-8680, Japan

preliminary version, June 28, 2009

Abstract

We introduce new polynomial invariants of a finite-dimensional semisimple and cosemisimple Hopf algebra A over a field \mathbf{k} by using the braiding structures of A . We investigate basic properties of the polynomial invariants including stability under extension of the base field. Furthermore, we show that our polynomial invariants are indeed tensor invariants of the representation category of A , and recognize the difference of the representation category and the representation ring of A . Actually, by computing and comparing polynomial invariants, we find new examples of pairs of Hopf algebras whose representation rings are isomorphic, but representation categories are distinct.

Mathematics Subject Classifications (2000): 16W30, 18D10, 19A49

1 Introduction

In representation theory of Hopf algebras over a field \mathbf{k} it is a fundamental problem to know conditions for that the representation categories of two given Hopf algebras are equivalent as (abstract) \mathbf{k} -linear monoidal categories. A complete answer for this is given by Schauenburg [27, 29]. He introduced a notion of bi-Galois extensions, and showed that the monoidal equivalences of comodule categories over Hopf algebras are classified by bi-Galois extensions of the base field \mathbf{k} . If the Hopf algebra A is of finite dimension, then this is equivalent to that A and B are cocycle deformations of each other, which are introduced by Doi [3]. Many researchers have been successful to determine the bi-Galois objects and the cocycle deformations for various special families of Hopf algebras, e.g. [16, 4, 28, 18]. However, it is very difficult to do so in general.

In this paper we introduce a new family of invariants of a semisimple and cosemisimple Hopf algebra of finite dimension by using the braiding structures of it, and show that our invariants are useful for examining whether the representation categories of two such Hopf algebras are monoidal equivalent or not.

*E-mail address: wakui@ipcku.kansai-u.ac.jp

The basic idea of our method is to utilize quantum invariants of low-dimensional manifolds, that are topological invariants defined by using quantum groups, namely, Hopf algebras with braiding structures. In contrast to most of current investigations on quantum invariants in which topological problems of low-dimensional manifolds are studied under a fixed Hopf algebra, in this research, we fix a framed knot or link, and study on representation categories of Hopf algebras. In particular, in this paper, by use of quantum invariants of the unknot with $(+1)$ -framing we introduce polynomials $P_A^{(d)}(x)$ ($d = 1, 2, \dots$) as invariants of a finite-dimensional semisimple and cosemisimple Hopf algebra A over \mathbf{k} . For each positive integer d the polynomial $P_A^{(d)}(x)$ is defined by

$$P_A^{(d)}(x) = \prod_{i=1}^t \prod_{R: \text{braidings of } A} \left(x - \frac{\dim_R M_i}{\dim M_i} \right) \in \mathbf{k}[x],$$

where $\{M_1, \dots, M_t\}$ is a full set of non-isomorphic absolutely simple left A -modules of dimension d (so, $\dim M_i = d$ for all i), and $\dim_R M_i \in \mathbf{k}$ is the quantum invariant of unknot with $(+1)$ -framing and colored by M_i . In algebraic language, $\dim_R M_i$ is the category-theoretic rank of M_i in the left rigid braided monoidal category $({}_A\mathbb{M}^{\text{f.d.}}, c_R)$ [15], where ${}_A\mathbb{M}^{\text{f.d.}}$ is the monoidal category of finite-dimensional left A -modules and A -linear maps, and c_R is the braiding of ${}_A\mathbb{M}^{\text{f.d.}}$ determined by R .

Provided that the polynomial $P_A^{(d)}(x)$ is not a constant, all roots of $P_A^{(d)}(x)$ are n -th roots of unity for some positive integer n . Furthermore the polynomial has nice properties such as integer property and stability under extension of the base field as follows. All coefficients of the polynomial are integers if \mathbf{k} is a finite Galois extension of the rational number field \mathbb{Q} , and A is a scalar extension of some finite-dimensional semisimple Hopf algebra over \mathbb{Q} . The polynomial is stabilized by taking some suitable extension of the base field, more precisely, there is a finite separable field extension L/\mathbf{k} so that $P_{A^L}^{(d)}(x) = P_A^{(d)}(x)$ for any field extension E/L .

It is more interesting to note that our polynomial invariants are indeed invariants of representation categories of Hopf algebras, and recognize the difference of representation categories and representation rings of that. In general, if representation categories of two finite-dimensional semisimple Hopf algebras are equivalent as monoidal categories, then their representation rings are isomorphic. However, the converse is not true. For example, by Tambara and Yamagami [32], and also Masuoka [18], it has proved that if the characteristic of \mathbf{k} is 0 or $p > 2$, then three non-commutative and semisimple Hopf algebras $\mathbf{k}[D_8]$, $\mathbf{k}[Q_8]$, K_8 of dimension 8 have the same representation ring, but their representation categories are not mutually equivalent, where D_8 is the dihedral group of order 8, Q_8 is the quaternion group, and K_8 is the Kac-Paljutkin algebra [9, 17]. This result is confirmed by our polynomial invariants, again. Moreover, by computing and comparing polynomial invariants we find new examples of pairs of Hopf algebras, whose representation rings are the same, but representation categories are distinct.

This paper consists of six sections in total, and they are divided into two parts except this introduction: from Section 2 to Section 4 the definition and general properties of the polynomial invariants are discussed, and from Section 5 to the final section several concrete examples are computed, and applications are described. Detailed contents are as follows. In Section 2 we

introduce the definition of our polynomial invariants of a semisimple and cosemisimple Hopf algebra of finite dimension. It is proved that the polynomial invariants are indeed invariants of the representation category of such a Hopf algebra. In Section 3 some basic properties of polynomial invariants are studied. It is shown that the polynomial invariants have nice properties such as integer property and stability under extension of the base field. In Section 4 by dualizing the method of construction of our polynomial invariants, we state a formula to compute them in terms of coalgebraic and comodule-categorical language. In Section 5 we demonstrate computations of polynomial invariants for several Hopf algebras including the Hopf algebras $A_{Nn}^{+\lambda}$ (N is odd, and $\lambda = \pm 1$), that are introduced by Satoshi Suzuki [30], and by comparing them we re-prove the Tambara, Yamagami and Masuoka's result as previously mentioned, and also find some pairs of Hopf algebras, whose representation rings are isomorphic, but representation categories are distinct. In the final section as an appendix we determine the structures of representation rings of the Hopf algebras $A_{Nn}^{+\lambda}$, and determine when they are self-dual, which are used in Section 5.

Throughout this paper, we use the notation \otimes instead of $\otimes_{\mathbf{k}}$, and denote by $\text{ch}(\mathbf{k})$ the characteristic of the field \mathbf{k} . For a Hopf algebra A , denoted by Δ , ε and S are the coproduct, the counit, and the antipode of A , respectively, and $G(A)$ is the group consisting of the group-like elements in A , and A^{cop} is the resulting Hopf algebra from A by replacing Δ by the opposite coproduct Δ^{cop} . We write ${}_A\mathbb{M}$ for the \mathbf{k} -linear monoidal category whose objects are left A -modules and morphisms are left A -linear maps, and write ${}^A\mathbb{M}$ for the \mathbf{k} -linear monoidal category whose objects are left A -comodules and morphisms are left A -colinear maps. For general references on Hopf algebras we refer to Abe's book [1], Montgomery's book [19] and Sweedler's book [31]. For general references on monoidal categories we refer to MacLane's book [14] and Joyal and Street's paper [8].

2 Definition of polynomial invariants

In this section we introduce a new family of invariants of a semisimple and cosemisimple Hopf algebra of finite dimension over an arbitrary field. They are given by polynomials derived from the quasitriangular structures of the Hopf algebra. By the method of construction of the polynomials they also become invariants under monoidal equivalence of representation categories of Hopf algebras.

Let us recall the definition of a quasitriangular Hopf algebra [5]. Let A be a Hopf algebra over a field \mathbf{k} , and $R \in A \otimes A$ an invertible element. The pair (A, R) is said to be a *quasitriangular Hopf algebra*, and R is said to be a *universal R -matrix* of A , if the following three conditions are satisfied:

- $\Delta^{\text{cop}}(a) = R \cdot \Delta(a) \cdot R^{-1}$ for all $a \in A$,
- $(\Delta \otimes \text{id})(R) = R_{13}R_{23}$,
- $(\text{id} \otimes \Delta)(R) = R_{13}R_{12}$.

Here $\Delta^{\text{cop}} = T \circ \Delta$, $T : A \otimes A \longrightarrow A \otimes A$, $T(a \otimes b) = b \otimes a$, and $R_{ij} \in A \otimes A \otimes A$ is given by $R_{12} = R \otimes 1$, $R_{23} = 1 \otimes R$, $R_{13} = (T \otimes \text{id})(R_{23}) = (\text{id} \otimes T)(R_{12})$.

If $R = \sum_i \alpha_i \otimes \beta_i$ is a universal R -matrix of A , then the element $u = \sum_i S(\beta_i) \alpha_i$ of A is invertible, and it has the following properties:

$$(i) \ S^2(a) = uau^{-1} \text{ for all } a \in A,$$

$$(ii) \ S(u) = \sum_i \alpha_i S(\beta_i).$$

The above element u is called the *Drinfel'd element* associated to R . If A is semisimple and cosemisimple of finite dimension, then the Drinfel'd element u belongs to the center of A by the property (i) and $S^2 = \text{id}_A$ [7, Corollary 3.2(i)].

Let (A, R) be a quasitriangular Hopf algebra over a field \mathbf{k} and u the Drinfel'd element associated to R . For a finite-dimensional left A -module M , we denote by $\underline{\dim}_R M$ the trace of the left action of u on M , and call it the R -dimension of M . The R -dimension $\underline{\dim}_R M$ is a special case of the braided dimension of M in the left rigid braided monoidal category $({}_A\mathbb{M}^{\text{f.d.}}, c_R)$ (see Section 4 for the definition of braided dimensions).

To define polynomial invariants, we use the following result established by Etingof and Gelaki [7].

Theorem 2.1 (Etingof and Gelaki). *Let A be a cosemisimple Hopf algebra of finite dimension over a field \mathbf{k} . Then*

- (1) *the set of universal R -matrices $\text{Braid}(A)$ is finite,*
- (2) *provided that A is semisimple, $(\dim M)1_{\mathbf{k}} \neq 0$ for any absolutely simple left A -module M .*

Remark 2.2. The proof of Part (1) was given in [7, Corollary 1.5] (see also Remark 3.12 in Section 3). In an extra case such as characteristic 0 or positive characteristic with some additional assumptions, it was proved by Radford [23, Theorem 1]. The proof of Part (2) was given in [7, Corollary 3.2(ii)]. The Etingof and Gelaki's proof is based on a Larson's result [10, Theorem 2.8], that is the same as Part (2) with the assumption $S^2 = \text{id}_A$.

Let A be a semisimple and cosemisimple Hopf algebra of finite dimension over a field \mathbf{k} . For a finite-dimensional left A -module M with $(\dim M)1_{\mathbf{k}} \neq 0$, we have a polynomial

$$P_{A,M}(x) := \prod_{R \in \text{Braid}(A)} \left(x - \frac{\underline{\dim}_R M}{\dim M} \right) \in \mathbf{k}[x].$$

Furthermore, for each positive integer d a polynomial $P_A^{(d)}(x)$ is defined by

$$P_A^{(d)}(x) := \prod_{i=1}^t P_{A,M_i}(x) \in \mathbf{k}[x],$$

where $\{M_1, \dots, M_t\}$ is a full set of non-isomorphic absolutely simple left A -modules of dimension d . Here, if there is no absolutely simple left A -module of dimension d , then we set $P_A^{(d)}(x) = 1$.

Example 2.3. Let $G = C_m$ be the cyclic group of order m generated by g , and let \mathbf{k} be a field whose characteristic does not divide m . Suppose that \mathbf{k} contains a primitive m -th root of unity ω . Then any universal R -matrix of the group Hopf algebra $\mathbf{k}[C_m]$ is given by

$$R_d = \sum_{i,j=0}^{m-1} \omega^{dij} E_i \otimes E_j \quad (d = 0, 1, \dots, m-1), \quad (2.1)$$

where $E_i = \frac{1}{m} \sum_{j=0}^{m-1} \omega^{-ij} g^j$ (see [24] for example). Let $M_j = \mathbf{k}$ be the (absolutely) simple left $\mathbf{k}[C_m]$ -module equipped with the action $\chi_j(g^p) = \omega^{jp}$ ($p = 0, 1, \dots, m-1$). For each d and i , then $\dim_{R_d} M_j = \omega^{-dj^2}$ since the Drinfel'd element u_d of R_d is given by $u_d = \sum_{i=0}^{m-1} \omega^{-di^2} E_i$. Thus we have

$$P_{\mathbf{k}[C_m]}^{(1)}(x) = \prod_{d,j=0}^{m-1} (x - \omega^{-dj^2}) = \prod_{j=0}^{m-1} (x^{\frac{m}{\gcd(j^2, m)}} - 1)^{\gcd(j^2, m)}.$$

Two Hopf algebras A and B over \mathbf{k} are said to be *monoidally Morita equivalent* if monoidal categories ${}_A\mathbb{M}$ and ${}_B\mathbb{M}$ are equivalent as \mathbf{k} -linear monoidal categories.

Lemma 2.4. *Let A and B be Hopf algebras of finite dimension over \mathbf{k} . If a \mathbf{k} -linear monoidal functor $F : {}_A\mathbb{M} \longrightarrow {}_B\mathbb{M}$ is an equivalence between monoidal categories, then $\dim M = \dim F(M)$ for any finite-dimensional left A -module M .*

Proof. We set $H := A^{*\text{cop}}$, $L := B^{*\text{cop}}$. Then the monoidal categories ${}_A\mathbb{M}$ and ${}_B\mathbb{M}$ can be identified with the monoidal categories ${}^H\mathbb{M}$, ${}^L\mathbb{M}$, respectively, and F can be regarded as a \mathbf{k} -linear monoidal functor from ${}^H\mathbb{M}$ to ${}^L\mathbb{M}$. By a Schauenburg's result [27, Corollary 5.7], there is an (L, H) -bi-Galois object X and a monoidal natural equivalence $\xi : F \Longrightarrow F_0$, where F_0 is the \mathbf{k} -linear monoidal functor defined by

$$F_0 : {}^H\mathbb{M} \longrightarrow {}^L\mathbb{M}, \quad M \longmapsto X \square_H M,$$

and \square_H denotes the cotensor product over H . Thus for a finite-dimensional left A -module M , we have a \mathbf{k} -linear isomorphism

$$\begin{aligned} X \otimes F(M) &\cong X \otimes (X \square_H M) \cong (X \otimes X) \square_H M \\ &\cong (X \otimes H) \square_H M \cong X \otimes (H \square_H M) \cong X \otimes M. \end{aligned}$$

This implies that $\dim F(M) = \dim M$. □

Lemma 2.5. *Let A and B be Hopf algebras of finite dimension over \mathbf{k} . If a \mathbf{k} -linear monoidal functor $(F, \phi, \omega) : {}_A\mathbb{M} \longrightarrow {}_B\mathbb{M}$ is an equivalence between monoidal categories, then there is a bijection $\Phi : \underline{\text{Braid}}(A) \longrightarrow \underline{\text{Braid}}(B)$ such that for a finite-dimensional left A -module M and a universal R -matrix $R \in \underline{\text{Braid}}(A)$,*

$$\dim_R M = \dim_{\Phi(R)} F(M).$$

Proof. Let $(G, \phi', \omega') : {}_B\mathbb{M} \longrightarrow {}_A\mathbb{M}$ be a quasi-inverse of (F, ϕ, ω) . Then there are \mathbf{k} -linear monoidal natural transformations $\varphi : (F, \phi, \omega) \circ (G, \phi', \omega') \Longrightarrow 1_{{}_B\mathbb{M}}$ and $\psi : (G, \phi', \omega') \circ (F, \phi, \omega) \Longrightarrow 1_{{}_A\mathbb{M}}$, where 1_ν stands for the identity functor on $\nu = {}_A\mathbb{M}, {}_B\mathbb{M}$.

A universal R -matrix $R = \sum_i \alpha_i \otimes \beta_i$ of A defines a braiding $c = \{c_{M,N} : M \otimes N \longrightarrow N \otimes M\}_{M,N \in {}_A\mathbb{M}}$ consisting of A -linear isomorphisms

$$c_{M,N}(m \otimes n) = \sum_i \beta_i n \otimes \alpha_i m \quad (m \in M, n \in N).$$

The braiding c gives rise to a braiding c' of ${}_B\mathbb{M}$, which consists of B -linear isomorphisms $c'_{P,Q} : P \otimes Q \longrightarrow Q \otimes P$ ($P, Q \in {}_B\mathbb{M}$) such that the following diagram commutes.

$$\begin{array}{ccc} P \otimes Q & \xrightarrow{c'_{P,Q}} & Q \otimes P \\ \varphi(P) \otimes \varphi(Q) \uparrow & & \uparrow \varphi(Q) \otimes \varphi(P) \\ FG(P) \otimes FG(Q) & & FG(Q) \otimes FG(P) \\ \phi_{G(P), G(Q)} \downarrow & & \downarrow \phi_{G(Q), G(P)} \\ F(G(P) \otimes G(Q)) & \xrightarrow{F(c_{G(P), G(Q)})} & F(G(Q) \otimes G(P)) \end{array}$$

Then $\Phi(R) := (T \circ c'_{B,B})(1)$ is a universal R -matrix of B , where $T : B \otimes B \longrightarrow B \otimes B$ is defined by $T(a \otimes b) = b \otimes a$ ($a, b \in B$). It is easy to see from definition that the map $\Phi : \underline{\text{Braid}}(A) \longrightarrow \underline{\text{Braid}}(B)$ defined as above is bijective.

Let M be a finite-dimensional left A -module, and e_M and n_M the evaluation and coevaluation morphisms defined by

$$\begin{aligned} e_M : M^* \otimes M &\longrightarrow \mathbf{k}, \quad e_M(f \otimes m) = f(m) \quad (f \in M^*, m \in M), \\ n_M : \mathbf{k} &\longrightarrow M \otimes M^*, \quad n_M(1) = \sum_i e_i \otimes e_i^* \quad (\text{the canonical element}). \end{aligned}$$

Then $e_M \circ c_{M,M^*} \circ n_M = (\underline{\dim}_R M) \text{id}_{\mathbf{k}}$. So, we may identify $\underline{\dim}_R M = e_M \circ c_{M,M^*} \circ n_M$. We set $e'_{F(M)} := \omega^{-1} \circ F(e_M) \circ \phi_{M^*, M}$ and $n'_{F(M)} := \phi_{M, M^*}^{-1} \circ F(n_M) \circ \omega$. Then $(F(M^*), e'_{F(M)}, n'_{F(M)})$ is a left dual for $F(M)$. Since the \mathbf{k} -linear monoidal functor (F, ϕ, ω) becomes a braided monoidal functor from $({}_A\mathbb{M}, c)$ to $({}_B\mathbb{M}, c')$, it follows that

$$\begin{aligned} \underline{\dim}_{\Phi(R)} F(M) &= e'_{F(M)} \circ c'_{F(M), F(M^*)} \circ n'_{F(M)} \\ &= \omega^{-1} \circ F(e_M \circ c_{M,M^*} \circ n_M) \circ \omega \\ &= (\underline{\dim}_R M) \omega^{-1} \circ F(\text{id}_{\mathbf{k}}) \circ \omega \\ &= \underline{\dim}_R M. \end{aligned}$$

□

Theorem 2.6. *Let A and B be semisimple and cosemisimple Hopf algebras of finite dimension over \mathbf{k} . If A and B are monoidally Morita equivalent, then $P_A^{(d)}(x) = P_B^{(d)}(x)$ for any positive integer d .*

Proof. Let $F : {}_A\mathbb{M} \longrightarrow {}_B\mathbb{M}$ be a \mathbf{k} -linear monoidal functor which gives an equivalence of monoidal categories, and let us consider the bijection $\Phi : \underline{\text{Braid}}(A) \longrightarrow \underline{\text{Braid}}(B)$ given as in the proof of Lemma 2.4.

Let M be an absolutely simple left A -module. Then $F(M)$ is also an absolutely simple left B -module, and by Lemma 2.4 and Lemma 2.5 we have

$$P_{A,M}(x) = P_{B,F(M)}(x). \quad (2.2)$$

Let $\{M_1, \dots, M_t\}$ be a full set of non-isomorphic absolutely simple left A -modules of dimension d . Then $\{F(M_1), \dots, F(M_t)\}$ is also a full set of non-isomorphic absolutely simple left B -modules of dimension d . Applying the equation (2.2) to $M = M_i$ ($i = 1, \dots, t$), and taking the product of them, we have $P_A^{(d)}(x) = P_B^{(d)}(x)$. \square

Remark 2.7. Our polynomial invariants are useful only if a semisimple and cosemisimple Hopf algebra has a quasitriangular structure. However, by considering the polynomial invariants of the Drinfeld double of it we have monoidal invariants of the original (arbitrary) semisimple Hopf algebra of finite dimension.

3 Properties of polynomial invariants

In this section we investigate basic properties of the polynomial invariants $P_A^{(d)}(x)$ ($d = 1, 2, \dots$) defined in Section 2. This section consists of two subsections. In the subsection 3.1 we prove that all coefficients of $P_A^{(d)}(x)$ are integers if \mathbf{k} is a finite Galois extension of \mathbb{Q} , and A is a scalar extension of some finite-dimensional semisimple Hopf algebra over \mathbb{Q} . In the subsection 3.2 we prove that $P_A^{(d)}(x)$ is stabilized by taking some suitable extension of the base field, more precisely, there is a finite separable field extension L/\mathbf{k} so that $P_{A^E}^{(d)}(x) = P_A^{(d)}(x)$ for any field extension E/L .

3.1 Integer property of polynomial invariants

First of all, we show that the coefficients of $P_A^{(d)}(x)$ lie in the integral closure of the prime ring of the base field of A . To do this we need the following lemma.

Lemma 3.1. *Let (A, R) be a quasitriangular Hopf algebra over \mathbf{k} and u the Drinfel'd element associated to R . If A is semisimple and cosemisimple, then $u^{(\dim A)^3} = 1$.*

Proof. Let us consider the following subHopf algebras of A :

$$B = \{ (\alpha \otimes \text{id})(R) \mid \alpha \in A^* \}, \quad H = \{ (\text{id} \otimes \alpha)(R) \mid \alpha \in A^* \}.$$

By [25, Proposition 2], the Hopf algebra B is isomorphic to the Hopf algebra $H^{*\text{cop}}$. Let $(D(H), \mathcal{R})$ be the Drinfel'd double of H . By [25, Theorem 2], there is a homomorphism $F :$

$(D(H), \mathcal{R}) \longrightarrow (A, R)$ of quasitriangular Hopf algebras. It follows that the Drinfel'd element \tilde{u} of $(D(H), \mathcal{R})$ satisfies $F(\tilde{u}) = u$. Since A is semisimple, subHopf algebras H and $H^{*\text{cop}} \cong B$ are also semisimple [13, Corollary 2.5]. Thus H is semisimple and cosemisimple. So, we have $\tilde{u}^{(\dim H)^3} = 1$ by [6, Theorem 2.5 & Theorem 4.3], and $u^{(\dim H)^3} = 1$. Since $\dim A$ is divided by $\dim H$ [25, Proposition 2], the equation $u^{(\dim A)^3} = 1$ is obtained. \square

For a field K , let Z_K denote the integral closure of the prime ring of K , that is, if the characteristic of K is 0, then Z_K is the ring of algebraic integers in K , and if the characteristic of K is $p > 0$, then Z_K is the algebraic closure of the prime field \mathbb{F}_p in K .

Lemma 3.2. *Let (H, R) be a semisimple and cosemisimple quasitriangular Hopf algebra over a field K . If M is an absolutely simple left H -module, then (by Theorem 2.1 $(\dim M)1_K \neq 0$ and,)*

$$\left(\frac{\dim_R M}{\dim M} \right)^{(\dim H)^3} = 1.$$

In particular, $\frac{\dim_R M}{\dim M} \in Z_K$.

Proof. The Drinfel'd element u of (H, R) belongs to the center of H since H is semisimple and cosemisimple. Thus the left action $\underline{u}_M : M \longrightarrow M$ of u is a left H -endomorphism. Since M is absolutely simple, \underline{u}_M is a scalar multiple of the identity morphism, so it can be written as $\underline{u}_M = \omega_M \text{id}_M$ for some $\omega_M \in K$. Then by Lemma 3.1 we have

$$\dim M = \text{Tr}(\underline{u}_M^{(\dim H)^3}) = \omega_M^{(\dim H)^3} \text{Tr}(\text{id}_M) = \omega_M^{(\dim H)^3} \dim M.$$

Thus $\omega_M^{(\dim H)^3} = 1$. This implies that $\omega_M = \frac{\dim_R M}{\dim M}$ belongs to Z_K . \square

Form Lemma 3.2, we have the following immediately.

Proposition 3.3. *Let H be a semisimple and cosemisimple Hopf algebra of finite dimension over a field K . Then for any absolutely simple left H -module M , the coefficients of the polynomial $P_{H,M}(x)$ are in Z_K . Therefore, $P_H^{(d)}(x) \in Z_K[x]$ for any positive integer d .*

Now, we will examine relationship between polynomial invariants and Galois extensions of fields. Let K/\mathbf{k} be a field extension, and let $\text{Aut}(K/\mathbf{k})$ denote the automorphism group of K/\mathbf{k} . For a K -linear space M and $\sigma \in \text{Aut}(K/\mathbf{k})$, a K -linear space ${}^\sigma M$ is defined as follows :

- (i) ${}^\sigma M = M$ as additive groups,
- (ii) the action \star of K on ${}^\sigma M$ is given by

$$c \star m := \sigma(c) \cdot m \quad (c \in K, m \in M), \quad (3.1)$$

where \cdot in the right-hand side stands for the original action of K on M .

For a K -linear map $f : M \longrightarrow N$ and $\sigma \in \text{Aut}(K/\mathbf{k})$, we have

$$f(c \star m) = f(\sigma(c) \cdot m) = \sigma(c) \cdot f(m) = c \star f(m) \quad (c \in K, m \in M),$$

thus f can be regarded as a K -linear map from ${}^\sigma M$ to ${}^\sigma N$. We denote by ${}^\sigma f$ the K -linear map $f : {}^\sigma M \longrightarrow {}^\sigma N$.

The monoidal category ${}_K \mathbb{M}$ of K -linear spaces and K -linear maps has a canonical braiding, which is given by usual twist maps. For an automorphism $\sigma \in \text{Aut}(K/\mathbf{k})$, the functor

$${}^\sigma F : {}_K \mathbb{M} \longrightarrow {}_K \mathbb{M}, \quad M \longmapsto {}^\sigma M, \quad f \longmapsto {}^\sigma f \quad (3.2)$$

gives a K -linear braided monoidal functor. Since ${}^\sigma F \circ {}^\tau F = {}^{\sigma\tau} F$ for all $\sigma, \tau \in \text{Aut}(K/\mathbf{k})$, the functor ${}^\sigma F : {}_K \mathbb{M} \longrightarrow {}_K \mathbb{M}$ gives an isomorphism of K -linear braided monoidal categories. In general, a K -linear braided monoidal functor $F : {}_K \mathbb{M} \longrightarrow {}_K \mathbb{M}$ maps a Hopf algebra to a Hopf algebra. So, for a Hopf algebra H over K and an automorphism $\sigma \in \text{Aut}(K/\mathbf{k})$, ${}^\sigma H$ also a Hopf algebra over K . The Hopf algebra structure of ${}^\sigma H$ is the same as that of H with the exception that the action of K on ${}^\sigma H$ is given by (3.1), and the counit $\varepsilon_{{}^\sigma H}$ of ${}^\sigma H$ is given by $\varepsilon_{{}^\sigma H} = \sigma^{-1} \circ \varepsilon_H$.

Lemma 3.4. *Let K/\mathbf{k} be a field extension, and H a Hopf algebra over K . Let $R \in H \otimes_K H$ be a universal R -matrix of H , and $\sigma \in \text{Aut}(K/\mathbf{k})$. Then*

- (1) *R is also a universal R -matrix of ${}^\sigma H$. We write ${}^\sigma R$ for this universal R -matrix of ${}^\sigma H$.*
- (2) *the Drinfel'd element of the quasitriangular Hopf algebra $({}^\sigma H, {}^\sigma R)$ coincides with the Drinfel'd element of (H, R) .*
- (3) *for a finite-dimensional left H -module M , we have $\underline{\dim}_{{}^\sigma R} {}^\sigma M = \sigma^{-1}(\underline{\dim}_R M)$.*

Proof. Parts (1) and (2) follow from definition. We show Part (3). Let $u \in H$ be the Drinfel'd element of (H, R) . By Part (2), u is also the Drinfel'd element of $({}^\sigma H, {}^\sigma R)$. Let $\{e_i\}_{i=1}^n$ be a basis of M over K , and write

$$u \cdot e_i = \sum_{j=1}^n a_{ji} e_j \quad (a_{ji} \in K).$$

Then $u \cdot e_i = \sum_{j=1}^n \sigma^{-1}(a_{ji}) \star e_j$, and whence

$$\underline{\dim}_{{}^\sigma R} {}^\sigma M = \sum_{i=1}^n \sigma^{-1}(a_{ii}) = \sigma^{-1}\left(\sum_{i=1}^n a_{ii}\right) = \sigma^{-1}(\underline{\dim}_R M).$$

□

For a field automorphism $\sigma : K \longrightarrow K$ and a polynomial $P(x) = c_0 + c_1 x + \cdots + c_m x^m$ ($c_i \in K$, $i = 1, \dots, m$), we define $\sigma \cdot P(x) \in K[x]$ by

$$\sigma \cdot P(x) := \sigma(c_0) + \sigma(c_1)x + \cdots + \sigma(c_m)x^m.$$

Lemma 3.5. *Let K/\mathbf{k} be a field extension, and H a semisimple and cosemisimple Hopf algebra over K of finite dimension. If M is a finite-dimensional left H -module such that $(\dim M)1_K \neq 0$, then for an automorphism $\sigma \in \text{Aut}(K/\mathbf{k})$ we have*

$$\sigma^{-1} \cdot P_{H,M}(x) = P_{\sigma H, \sigma M}(x).$$

Proof. Setting $N = \sigma M$, by Lemma 3.4(3) we have

$$\begin{aligned} \sigma^{-1} \cdot P_{H,M}(x) &= \prod_{R \in \underline{\text{Braid}}(H)} \left(x - \sigma^{-1} \left(\frac{\dim_R M}{\dim M} \right) \right) \\ &= \prod_{R \in \underline{\text{Braid}}(H)} \left(x - \frac{\sigma^{-1}(\dim_R M)}{\dim M} \right) \\ &= \prod_{R \in \underline{\text{Braid}}(H)} \left(x - \frac{\dim_{\sigma R} N}{\dim N} \right) \\ &\stackrel{(*)}{=} P_{\sigma H, N}(x). \end{aligned}$$

Here, the last equation (*) follows from what the map $\underline{\text{Braid}}(H) \longrightarrow \underline{\text{Braid}}(\sigma H)$, $R \longmapsto \sigma R$ is bijective by Lemma 3.4(1). \square

Let A be a Hopf algebra over a field \mathbf{k} , and K an extension field of \mathbf{k} . Then $A^K = A \otimes K$ becomes a Hopf algebra over K , and the automorphism group $\text{Aut}(K/\mathbf{k})$ acts on A^K as follows:

$$\sigma \cdot (a \otimes c) = a \otimes \sigma(c) \quad (\sigma \in \text{Aut}(K/\mathbf{k}), a \in A, c \in K). \quad (3.3)$$

We set $H = A^K$. Then for each $\sigma \in \text{Aut}(K/\mathbf{k})$ the left action on H given by (3.3) defines a Hopf algebra isomorphism from H to σH , denoted by $\tilde{\sigma} : H \longrightarrow \sigma H$. Furthermore, we see that if R is a universal R -matrix of H , then $\tilde{\sigma}$ becomes a homomorphism of quasitriangular Hopf algebras from (H, R) to $(\sigma H, \sigma R)$. Thus $\text{Aut}(K/\mathbf{k})$ acts on $\underline{\text{Braid}}(H)$ from the right by

$$R \in \underline{\text{Braid}}(H) \longmapsto (\tilde{\sigma}^{-1} \otimes_K \tilde{\sigma}^{-1})(\sigma R) \in \underline{\text{Braid}}(H).$$

Theorem 3.6. *Let K/\mathbf{k} be a finite Galois extension of fields, and A a semisimple and cosemisimple Hopf algebra over \mathbf{k} of finite dimension. Then $P_{A^K}^{(d)}(x) \in (\mathbf{k} \cap Z_K)[x]$ for each positive integer d .*

Proof. First of all, let us check to see that the Hopf algebra $H = A^K$ is semisimple and cosemisimple. Since the Hopf algebra A is semisimple, it is separable (see [19, Corollary 2.2.2]). Thus H is a semisimple Hopf algebra over K of finite dimension. Applying the same argument to the dual Hopf algebra A^* , we see that H is a cosemisimple Hopf algebra over K . Eventually, we see that H is semisimple and cosemisimple.

Let $\text{Irr}_0^{(d)}(H)$ denote the set of isomorphism classes $[M]$ of absolutely simple left H -modules M of dimension d , and set $t = \sharp \text{Irr}_0^{(d)}(H)$. If $t = 0$, then $P_H^{(d)}(x) = 1$, and hence $P_H^{(d)}(x) \in (\mathbf{k} \cap Z_K)[x]$.

Hereinafter, we consider the case of $t > 0$. For an automorphism $\sigma \in \text{Gal}(K/\mathbf{k})$, the map

$$\text{Irr}_0^{(d)}(H) \longrightarrow \text{Irr}_0^{(d)}(\sigma H), \quad [M] \longmapsto [\sigma M]$$

is bijective. Here, by Lemma 3.5 we have $\sigma^{-1} \cdot P_H^{(d)}(x) = P_{\sigma H}^{(d)}(x) = P_H^{(d)}(x)$, and we see that $P_H^{(d)}(x) \in \mathbf{k}[x]$. On the other hand, since $P_H^{(d)}(x) \in Z_K[x]$ by Proposition 3.3, it follows that $P_H^{(d)}(x) \in (\mathbf{k} \cap Z_K)[x]$. \square

As applications of the above theorem we have two corollaries.

Corollary 3.7. *Let K be a finite Galois extension field of \mathbb{Q} , and A a semisimple Hopf algebra over \mathbb{Q} of finite dimension. Then $P_{A^K}^{(d)}(x) \in \mathbb{Z}[x]$ for any positive integer d , where \mathbb{Z} denotes the rational integral ring.*

Proof. By [11] a finite-dimensional semisimple Hopf algebra over a field of characteristic 0 is cosemisimple. Thus the semisimple Hopf algebra A^K is cosemisimple. Since $\mathbb{Q} \cap Z_K = \mathbb{Z}$, by applying Theorem 3.6 we have $P_{A^K}^{(d)}(x) \in \mathbb{Z}[x]$. \square

Corollary 3.8. *Let Γ be a finite group, and K a finite Galois extension field of \mathbb{Q} . Then $P_{K[\Gamma]}^{(d)}(x) \in \mathbb{Z}[x]$ for any positive integer d .*

Proof. The group Hopf algebra $K[\Gamma]$ is isomorphic to the scalar extension of $\mathbb{Q}[\Gamma]$ by K . Since a group algebra over a field of characteristic 0 is semisimple, by Corollary 3.7 we have $P_{K[\Gamma]}^{(d)}(x) \in \mathbb{Z}[x]$ for any positive integer d . \square

3.2 Stability of polynomial invariants

Given a field extension K/\mathbf{k} , any universal R -matrix R of A can be regarded as a universal R -matrix of the scalar extension A^K in a natural way (see below for details). So, for an increasing sequence of finite extensions of fields $\mathbf{k} \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots$ we have an increasing sequence of sets of universal R -matrices $\underline{\text{Braid}}(A) \subset \underline{\text{Braid}}(A^{K_1}) \subset \underline{\text{Braid}}(A^{K_2}) \subset \cdots$. In this subsection we show that there is n such that $\underline{\text{Braid}}(A^{K_n}) = \underline{\text{Braid}}(A^{K_{n+1}}) = \cdots$. As an application, we prove that the polynomial invariants $P_A^{(d)}(x)$ ($d = 1, 2, \dots$) are stabilized by taking some suitable extension of the base field.

Let A be a Hopf algebra over a field \mathbf{k} , and L a commutative algebra over \mathbf{k} . Then $A^L = A \otimes L$ becomes a Hopf algebra over L . Furthermore, if $R = \sum_i \alpha_i \otimes \beta_i$ is a universal R -matrix of A , then

$$R^L = \sum_i (\alpha_i \otimes 1_{\mathbf{k}}) \otimes_L (\beta_i \otimes 1_{\mathbf{k}}) \in A^L \otimes_L A^L$$

is a universal R -matrix of A^L . Via the injection $\underline{\text{Braid}}(A) \longrightarrow \underline{\text{Braid}}(A^L)$ which sends R to R^L , we frequently regard $\underline{\text{Braid}}(A)$ as a subset of $\underline{\text{Braid}}(A^L)$.

Let $\underline{\mathbf{alg}}_{\mathbf{k}}$ denote the \mathbf{k} -additive category whose objects are commutative algebras over \mathbf{k} and morphisms are algebra maps between them. Let A and B be two Hopf algebras over \mathbf{k} . For a commutative algebra $L \in \underline{\mathbf{alg}}_{\mathbf{k}}$, we set

$$\mathrm{Hopf}_L(A^L, B^L) := \{ \text{the } L\text{-Hopf algebra maps } A^L \longrightarrow B^L \},$$

and for an algebra map $f : L_1 \longrightarrow L_2$ between commutative algebras $L_1, L_2 \in \underline{\mathbf{alg}}_{\mathbf{k}}$ and $\varphi \in \mathrm{Hopf}_{L_1}(A^{L_1}, B^{L_1})$ we define a map $f_*\varphi \in \mathrm{Hopf}_{L_2}(A^{L_2}, B^{L_2})$ by the composition:

$$\begin{aligned} A \otimes L_2 &\xrightarrow{\mathrm{id} \otimes \eta} A \otimes (L_1 \otimes L_2) \cong (A \otimes L_1) \otimes L_2 \xrightarrow{\varphi \otimes \mathrm{id}} (B \otimes L_1) \otimes L_2 \\ &\xrightarrow{\mathrm{id}_B \otimes f} (B \otimes L_2) \otimes L_2 \cong B \otimes (L_2 \otimes L_2) \xrightarrow{\mathrm{id} \otimes \mu_{L_2}} B \otimes L_2, \end{aligned}$$

where μ_{L_2} is the multiplication of L_2 , and $\eta : L_2 \longrightarrow L_1 \otimes L_2$ is the \mathbf{k} -algebra map defined by $\eta(y) = 1_{L_1} \otimes y$ ($y \in L_2$). This \mathbf{k} -linear map $f_*\varphi$ is directly defined by

$$(f_*\varphi)(a \otimes y) = \sum_i b_i \otimes f(x_i)y, \quad \left(\varphi(a \otimes 1_{L_1}) = \sum_i b_i \otimes x_i \right)$$

for all $a \in A$, $y \in L_2$. Let $\underline{\mathbf{Set}}$ denote the category whose objects are sets and morphisms are maps. Then we have a covariant functor $\mathbf{Hopf}(A, B) : \underline{\mathbf{alg}}_{\mathbf{k}} \longrightarrow \underline{\mathbf{Set}}$ such as

$$\begin{aligned} \text{for an object : } & L \longmapsto \mathrm{Hopf}_L(A^L, B^L), \\ \text{for a morphism : } & f \longmapsto \left(\mathbf{Hopf}(A, B)(f) : \varphi \longmapsto f_*\varphi \right). \end{aligned}$$

Provided that A and B are of finite dimension over \mathbf{k} , the functor $\mathbf{Hopf}(A, B)$ becomes an algebraic affine scheme over \mathbf{k} , that is, it is represented by a finitely generated commutative algebra $Z \in \underline{\mathbf{alg}}_{\mathbf{k}}$ [34, p.4–5 & p.58]. Furthermore, if A is semisimple, and B is cosemisimple, then the representing object Z is separable and of finite dimension, as the proof is given in the next proposition. This result is essentially proved by Etingof and Gelaki [7, Corollary 1.3], and in the case of $A = B$ and the affine group scheme $\mathbf{Aut}(A)$ the same result is proved by Waterhouse [35, Theorem 1] (see also [22, Corollary 6] and [23, Proposition 1] in case of characteristic 0 or positive characteristic with some additional assumptions).

Proposition 3.9. *Let A and B be Hopf algebras over \mathbf{k} of finite dimension. If A is semisimple, and B is cosemisimple, then the affine scheme $\mathbf{Hopf}(A, B)$ is finite etale, that is, a representing object $Z \in \underline{\mathbf{alg}}_{\mathbf{k}}$ of $\mathbf{Hopf}(A, B)$ is separable and of finite dimension.*

Proof. For two algebras A and B over \mathbf{k} , let $\mathrm{Alg}_{\mathbf{k}}(A, B)$ denote the set of the \mathbf{k} -algebra maps from A to B . Let $Z \in \underline{\mathbf{alg}}_{\mathbf{k}}$ be a representing object of the functor $\mathbf{Hopf}(A, B) : \underline{\mathbf{alg}}_{\mathbf{k}} \longrightarrow \underline{\mathbf{Set}}$. Since Z is finitely generated commutative, it is a Noetherian algebra over \mathbf{k} . Thus for an algebraically closed field $\bar{\mathbf{k}}$ which contains \mathbf{k} , the $\bar{\mathbf{k}}$ -algebra $\bar{Z} := Z \otimes \bar{\mathbf{k}}$ is also finitely generated commutative Noetherian. Then by Hilbert's Nullstellensatz the nilradical $\sqrt{0}$ of \bar{Z} coincides with the Jacobson radical $\mathrm{rad} \bar{Z}$, and the set of minimal prime ideals of \bar{Z} is finite. We will show

that any maximal ideal of \bar{Z} is a minimal prime ideal. To do this, it is enough to prove that $\mathfrak{m}^2 = \mathfrak{m}$ for any maximal ideal \mathfrak{m} of \bar{Z} . For $\phi \in \text{Alg}_{\bar{\mathbf{k}}}(\bar{Z}, \bar{\mathbf{k}})$, let us consider the ϕ -derivations

$$\text{Der}_{\phi}(\bar{Z}, \bar{\mathbf{k}}) = \{ \bar{\mathbf{k}}\text{-linear maps } \delta : \bar{Z} \longrightarrow \bar{\mathbf{k}} \mid \delta(\bar{z}\bar{z}') = \phi(\bar{z})\bar{z}' + \bar{z}\phi(\bar{z}') \text{ } (\bar{z}, \bar{z}' \in \bar{Z}) \}.$$

Considering the maximal ideal $\mathfrak{m}_{\phi} := \text{Ker } \phi$ of \bar{Z} , we have a $\bar{\mathbf{k}}$ -linear isomorphism $(\mathfrak{m}_{\phi}/\mathfrak{m}_{\phi}^2)^* \longrightarrow \text{Der}_{\phi}(\bar{Z}, \bar{\mathbf{k}})$. However, $\text{Der}_{\phi}(\bar{Z}, \bar{\mathbf{k}}) = 0$ by the proof of [7, Corollary 1.3]. So, we have $\mathfrak{m}_{\phi} = \mathfrak{m}_{\phi}^2$. It follows from Hilbert's Nullstellensatz that $\mathfrak{m} = \mathfrak{m}^2$ for any maximal ideal \mathfrak{m} of \bar{Z} . Since $\mathfrak{m}\bar{Z}_{\mathfrak{m}} = 0$, the localization $\bar{Z}_{\mathfrak{m}}$ becomes a field. This means that \mathfrak{m} is a minimal prime ideal of \bar{Z} .

From the above argument, it follows that the set of maximal ideals of \bar{Z} is finite. So, let $\mathfrak{m}_1, \dots, \mathfrak{m}_l$ be the maximal ideals of \bar{Z} . Then we have $\text{rad } \bar{Z} = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_l = \mathfrak{m}_1 \cdots \mathfrak{m}_l$. Since $\text{rad } \bar{Z} = \sqrt{0}$ is nilpotent, $(\text{rad } \bar{Z})^n = 0$ for a sufficiently large integer n . From this fact and $\mathfrak{m}_j^2 = \mathfrak{m}_j$ ($j = 1, \dots, l$), we see that $\text{rad } \bar{Z} = (\text{rad } \bar{Z})^n = 0$. Therefore, $\mathfrak{m}_1 \cdots \mathfrak{m}_l = 0$. This implies that the Noetherian algebra \bar{Z} is Artinian. Thus \bar{Z} is semisimple, that is, Z is separable. \square

For a Hopf algebra A over \mathbf{k} , the \mathbf{k} -linear space $\text{Hom}_{\mathbf{k}}(A^*, A)$ possesses a left A -module action \rightharpoonup and a right A -module action \leftharpoonup defined as follows.

$$\begin{aligned} (a \rightharpoonup f)(p) &= \sum a_{(1)} \langle p_{(1)}, a_{(2)} \rangle f(p_{(2)}), \\ (f \leftharpoonup a)(p) &= \sum f(p_{(1)}) \langle p_{(2)}, a_{(1)} \rangle a_{(2)} \end{aligned}$$

for $f \in \text{Hom}_{\mathbf{k}}(A^*, A)$, $p \in A^*$, $a \in A$. Here $\langle \cdot, \cdot \rangle$ denotes the natural pairing of A^* and A , and the sigma notation such as $\Delta(a) = \sum a_{(1)} \otimes a_{(2)}$ is used.

Lemma 3.10 ([24]). *Let A be a Hopf algebra over \mathbf{k} , and $F : A \otimes A \longrightarrow \text{Hom}_{\mathbf{k}}(A^*, A^{\text{cop}})$ be the injective \mathbf{k} -linear map defined by*

$$(F(a \otimes b))(p) = p(a)b \quad (a, b \in A, p \in A^*).$$

For an element $R \in A \otimes A$ we set $f = F(R) : A^ \longrightarrow A^{\text{cop}}$. Then*

- (1) *given $a \in A$, R satisfies $\Delta^{\text{cop}}(a) \cdot R = R \cdot \Delta(a)$ if and only if $a \rightharpoonup f = f \leftharpoonup a$,*
- (2) *R satisfies $(\Delta \otimes \text{id})(R) = R_{13}R_{23}$ and $(\varepsilon \otimes \text{id})(R) = 1$ if and only if f is an algebra map,*
- (3) *in the case where A is finite-dimensional, R satisfies $(\text{id} \otimes \Delta)(R) = R_{13}R_{12}$ and $(\text{id} \otimes \varepsilon)(R) = 1$ if and only if f is a coalgebra map.*

Therefore, if A is finite-dimensional, then the following are equivalent :

- (i) *R is a universal R -matrix of A ,*
- (ii) *f is a Hopf algebra map satisfying $a \rightharpoonup f = f \leftharpoonup a$ for all $a \in A$,*

and the restriction of F to $\underline{\text{Braid}}(A)$ defines an injection $j_A : \underline{\text{Braid}}(A) \longrightarrow \text{Hopf}_{\mathbf{k}}(A^, A^{\text{cop}})$.*

Combining Proposition 3.9 with Lemma 3.10, we have the following theorem.

Theorem 3.11. *Let A be a cosemisimple Hopf algebra over a field \mathbf{k} of finite dimension. Then there is a separable finite extension field L of \mathbf{k} such that $\underline{\mathbf{Braid}}(A^L) = \underline{\mathbf{Braid}}(A^E)$ for any field extension E/L .*

Proof. Since A is cosemisimple, the dual Hopf algebra A^* is semisimple. By Theorem 3.9, a representing object $Z \in \underline{\mathbf{alg}}_{\mathbf{k}}$ of the functor $\mathbf{Hopf}(A^*, A^{\text{cop}}) : \underline{\mathbf{alg}}_{\mathbf{k}} \rightarrow \underline{\mathbf{Set}}$ is separable and of finite dimension. So, we take a separable finite extension field L of \mathbf{k} which is a splitting field of Z . We set $H = A^L$, and consider the injective map $j_H : \underline{\mathbf{Braid}}(H) \rightarrow \mathbf{Hopf}_L(H^*, H^{\text{cop}})$ defined as in Lemma 3.10.

Let E be an extension field of L . Then the following diagram commutes for the inclusion $i : L \rightarrow E$.

$$\begin{array}{ccc}
\underline{\mathbf{Braid}}(H) & \xrightarrow{j_H} & \mathbf{Hopf}_L(H^*, H^{\text{cop}}) \\
\downarrow & & \wr \parallel \text{ (*2)} \\
& & \mathbf{Hopf}_L((A^*)^L, (A^{\text{cop}})^L) \\
& & \downarrow \mathbf{Hopf}(A^*, A^{\text{cop}})(i) \\
\underline{\mathbf{Braid}}(H^E) & & \mathbf{Hopf}_E((A^*)^E, (A^{\text{cop}})^E) \\
\wr \parallel \text{ (*1)} & & \wr \parallel \text{ (*3)} \\
\underline{\mathbf{Braid}}(A^E) & \xrightarrow{j_{A^E}} & \mathbf{Hopf}_E((A^E)^*, (A^E)^{\text{cop}})
\end{array}$$

Here, the arrow $\underline{\mathbf{Braid}}(H) \rightarrow \underline{\mathbf{Braid}}(H^E)$ of L.H.S. is expressing the map defined by $R \mapsto R^E$, and the isomorphisms marked with (*1), (*2), (*3) are induced from the Hopf algebra isomorphisms defined below, respectively:

$$\begin{aligned}
H^E &= (A^L) \otimes_L E \rightarrow A^E, & (a \otimes x) \otimes_L y &\mapsto a \otimes xy & (a \in A, x \in L, y \in E), \\
\iota_L : (A^*)^L &\rightarrow (A^L)^* = H^*, & \iota_L(q \otimes x) &: a \otimes x' \mapsto q(a)xx' & (q \in A^*, x, x' \in L), \\
\iota_E : (A^*)^E &\rightarrow (A^E)^*, & \iota_E(q \otimes y) &: a \otimes y' \mapsto q(a)yy' & (q \in A^*, y, y' \in E).
\end{aligned}$$

We will show that $\mathbf{Hopf}(A^*, A^{\text{cop}})(i)$ is bijective. Since Z is a representing object of $\mathbf{Hopf}(A^*, A^{\text{cop}})$, there are isomorphisms Φ_L and Φ_E such that the diagram

$$\begin{array}{ccc}
\text{Hopf}_L((A^*)^L, (A^{\text{cop}})^L) & \xrightarrow{\Phi_L} & \text{Alg}_{\mathbf{k}}(Z, L) \\
\downarrow \mathbf{Hopf}(A^*, A^{\text{cop}})(i) & & \downarrow \text{Alg}_{\mathbf{k}}(\text{id}_Z, i) \\
\text{Hopf}_E((A^*)^E, (A^{\text{cop}})^E) & \xrightarrow{\Phi_E} & \text{Alg}_{\mathbf{k}}(Z, E)
\end{array}$$

commutes. From this commutative diagram it is sufficient to show that $i_* := \text{Alg}_{\mathbf{k}}(\text{id}_Z, i) : \text{Alg}_{\mathbf{k}}(Z, L) \longrightarrow \text{Alg}_{\mathbf{k}}(Z, E)$ is bijective. It is clear that i_* is injective. To prove that i_* is surjective, let f be an algebra map in $\text{Alg}_{\mathbf{k}}(Z, E)$. Then $f(Z) \subset L$, since $Z \otimes L = L^{\oplus n}$ for some n as algebras over L , and E is a field. So, every algebra map $f \in \text{Alg}_{\mathbf{k}}(Z, E)$ defines an algebra map $g : Z \longrightarrow L$ such as $i_*(g) = f$. This means that $\text{Alg}_{\mathbf{k}}(\text{id}_Z, i) : \text{Alg}_{\mathbf{k}}(Z, L) \longrightarrow \text{Alg}_{\mathbf{k}}(Z, E)$ is surjective.

Next, we will show that $\mathbf{Hopf}(A^*, A^{\text{cop}})(i)$ preserves the actions \rightharpoonup and \leftharpoonup . Let φ be an element in $\text{Hopf}_L((A^*)^L, (A^{\text{cop}})^L)$. Then by using what $i_*\varphi = (\mathbf{Hopf}(A^*, A^{\text{cop}})(i))(\varphi)$ is given by

$$(i_*\varphi)(p \otimes y) = \varphi(p \otimes 1_L) \cdot (1_A \otimes y) \quad (p \in A^*, y \in E),$$

we have

$$\begin{aligned}
((a \otimes 1_L) \rightharpoonup \varphi)(p \otimes 1_L) &= (\varphi \leftharpoonup (a \otimes 1_L))(p \otimes 1_L) \\
&\iff ((a \otimes 1_E) \rightharpoonup i_*\varphi)(p \otimes 1_E) = (i_*\varphi \leftharpoonup (a \otimes 1_E))(p \otimes 1_E)
\end{aligned}$$

for all $a \in A$, $p \in A^*$. This implies that

$$\begin{aligned}
(a \otimes x) \rightharpoonup \varphi &= \varphi \leftharpoonup (a \otimes x) \text{ for all } a \in A \text{ and } x \in L \\
&\iff (a \otimes y) \rightharpoonup i_*\varphi = i_*\varphi \leftharpoonup (a \otimes y) \text{ for all } a \in A \text{ and } y \in E.
\end{aligned}$$

By Lemma 3.10, then we see that the map $\underline{\text{Braid}}(H) \longrightarrow \underline{\text{Braid}}(H^E)$, $R \longmapsto R^E$ is bijective. \square

Remark 3.12. Using Proposition 3.9 and Lemma 3.10, one can give a proof of Theorem 2.1(i) as follows (c.f. [7, Corollary 1.5]). Let A be a cosemisimple Hopf algebra over \mathbf{k} of finite dimension, and take L and H as in the proof of Theorem 3.11. Then by Proposition 3.9 the set $\text{Hopf}_L(H^*, H^{\text{cop}})$ is finite. It follows from the injectivity of j_H that the set $\underline{\text{Braid}}(H)$ is finite, too. Since $\underline{\text{Braid}}(A)$ can be identified with a subset of $\underline{\text{Braid}}(H)$, the set $\underline{\text{Braid}}(A)$ is also finite. This ends the proof of Theorem 2.1(i).

We note that for any field extension K/\mathbf{k} it is also true that $\underline{\text{Braid}}(A^K)$ is finite. Because, the scalar extension A^K is still cosemisimple.

Corollary 3.13. *Let A be a semisimple and cosemisimple Hopf algebra over a field \mathbf{k} of finite dimension. Then there is a separable finite extension field L of \mathbf{k} such that for any field extension E of L and for any positive integer d , $P_{A^E}^{(d)}(x) = P_{A^L}^{(d)}(x)$ in $E[x]$.*

Proof. Since A is separable by [19, Corollary 2.2.2], there is a finite separable extension field K of \mathbf{k} such that it is a splitting field of A . Then $H := A^K$ is a semisimple and cosemisimple Hopf algebra over K of finite dimension.

Let L be a separable finite extension field of K having the property in Theorem 3.11. Then for any field extension E/L and any absolutely simple left H^L -module M , the left $(H^L)^E$ -module M^E is absolutely simple, and the equation

$$P_{(H^L)^E, M^E}(x) = P_{H^L, M}(x) \quad (3.4)$$

holds in $E[x]$ since $\underline{\dim}_{R^E} M^E = \underline{\dim}_R M$ for all $R \in \underline{\text{Braid}}(H)$. Since K is a splitting field of H , if $\{M_1, \dots, M_t\}$ is a full set of non-isomorphic absolutely simple left H -modules of dimension d , then $\{M_1^E, \dots, M_t^E\}$ is a full set of non-isomorphic absolutely simple left H^E -modules of dimension d . From this fact and the equation (3.4), we have the equation

$$P_{(H^L)^E}^{(d)}(x) = \prod_{i=1}^t P_{(H^L)^E, (M_i^L)^E}(x) = \prod_{i=1}^t P_{H^L, M_i^L}(x) = P_{H^L}^{(d)}(x) \quad \text{in } E[x].$$

Since $(H^L)^E \cong H^E = (A^K)^E \cong A^E$ as Hopf algebras over E , we have $P_{(H^L)^E}^{(d)}(x) = P_{A^E}^{(d)}(x)$, and since $H^L = (A^K)^L \cong A^L$ as Hopf algebras over L , we have $P_{H^L}^{(d)}(x) = P_{A^L}^{(d)}(x)$. Thus the desired equation $P_{A^E}^{(d)}(x) = P_{A^L}^{(d)}(x)$ is obtained.

Finally, we remark that the extension L/\mathbf{k} is separable since two extensions L/K and K/\mathbf{k} are separable. \square

4 Dual formulas for polynomial invariants

In this section we give a formula to compute the polynomial invariants for a self-dual Hopf algebra of finite dimension in terms of the braidings of the dual Hopf algebra.

Let us recall the definition of a braiding of a Hopf algebra [3]. Let A be a Hopf algebra over a field \mathbf{k} , and let $\sigma : A \otimes A \longrightarrow \mathbf{k}$ be a \mathbf{k} -linear map that is invertible with respect to the convolution product. The pair (A, σ) is said to be a *braided Hopf algebra*, and σ is said to be a *braiding* of A if the following conditions are satisfied: for all $x, y, z \in A$

$$(B1) \quad \sum \sigma(x_{(1)}, y_{(1)}) x_{(2)} y_{(2)} = \sum \sigma(x_{(2)}, y_{(2)}) y_{(1)} x_{(1)},$$

$$(B2) \quad \sigma(xy, z) = \sum \sigma(x, z_{(1)}) \sigma(y, z_{(2)}),$$

$$(B3) \quad \sigma(x, yz) = \sum \sigma(x_{(1)}, z) \sigma(x_{(2)}, y).$$

Here, we use the sigma notation such as $\Delta(x) = \sum x_{(1)} \otimes x_{(2)}$ for $x \in A$. It is easy to see that any braiding σ of A satisfies

$$(B4) \quad \sigma(1_A, x) = \sigma(x, 1_A) = \varepsilon(x) \text{ for all } x \in A.$$

Let (A, σ) be a braided Hopf algebra over \mathbf{k} . Then the braiding σ defines a braiding c of the monoidal category \mathbb{M}^A consisting of right A -comodules and A -colinear maps as follows. For two right A -comodules V and W , a \mathbf{k} -linear isomorphism $c_{V,W} : V \otimes W \longrightarrow W \otimes V$ is defined by

$$c_{V,W}(v \otimes w) = \sum \sigma(v_{(1)}, w_{(1)}) w_{(0)} \otimes v_{(0)} \quad (v \in V, w \in W),$$

where we use the notations $\rho_V(v) = \sum v_{(0)} \otimes v_{(1)}$ and $\rho_W(w) = \sum w_{(0)} \otimes w_{(1)}$ for the given right coactions ρ_V and ρ_W of V and W , respectively. From the axiom of braiding (B1) – (B3), we see that $c_{V,W}$ is a right A -comodule isomorphism, and the collection $c = \{c_{V,W} : V \otimes W \longrightarrow W \otimes V\}_{V,W \in \mathbb{M}^A}$ gives a braiding of \mathbb{M}^A .

Let us consider the element in the braided Hopf algebra which plays a role of the Drinfel'd element in a quasitriangular Hopf algebra.

Lemma 4.1 ([3, Theorem 1.3] or [26, 3.3.2]). *Let (A, σ) be a braided Hopf algebra over \mathbf{k} , and define $\mu \in A^*$ by*

$$\mu(a) = \sum \sigma(a_{(2)}, S(a_{(1)})), \quad a \in A.$$

Then μ is convolution-invertible, and the following equation holds for any element $a \in A$:

$$S^2(a) = \sum \mu(a_{(1)}) \mu^{-1}(a_{(3)}) a_{(2)}.$$

The \mathbf{k} -linear functional μ is called the (dual) Drinfel'd element of (A, σ) .

Let $\mathcal{V} = (\mathcal{C}, \otimes, \mathbb{I}, a, r, l, c)$ be a left rigid braided monoidal category. For each object $X \in \mathcal{C}$ we choose a left dual X^* with an evaluation morphism $e_X : X^* \otimes X \longrightarrow \mathbb{I}$ and a coevaluation morphism $n_X : \mathbb{I} \longrightarrow X \otimes X^*$. Then for an endomorphism $f : X \longrightarrow X$ in \mathcal{C} , the braided trace of f in \mathcal{V} , denoted by $\underline{\text{Tr}}_c f$, is defined by the composition

$$\mathbb{I} \xrightarrow{n_X} X \otimes X^* \xrightarrow{f \otimes \text{id}} X \otimes X^* \xrightarrow{c_{X, X^*}} X^* \otimes X \xrightarrow{e_X} \mathbb{I}.$$

In particular, the braided trace of the identity morphism id_X is denoted by $\underline{\text{dim}}_c X$, and called the *braided dimension* of X in \mathcal{V} .

Applying this to the braided monoidal category (\mathbb{M}^A, c) constructed from a braiding $\sigma \in (A \otimes A)^*$, we have the following.

Lemma 4.2. *Let (A, σ) be a braided Hopf algebra over \mathbf{k} , and c the braiding of \mathbb{M}^A constructed from σ . Then for a finite-dimensional right A -comodule V , the braided dimension $\underline{\text{dim}}_c V$ is given by $\underline{\text{dim}}_\sigma V = \mu(\chi_V)$, where μ is the Drinfel'd element of (A, σ) , and χ_V is the character of the comodule V , which is defined by*

$$\chi_V := \sum_{i=1}^n (v_i^* \otimes \text{id}_C)(\rho_V(v_i)) \in C$$

by use of dual bases $\{v_i\}_{i=1}^n$ and $\{v_i^\}_{i=1}^n$.*

Lemma 4.3. *Let A be a Hopf algebra over \mathbf{k} of finite dimension, and $\iota : A^* \otimes A^* \longrightarrow (A \otimes A)^*$ is the canonical \mathbf{k} -linear isomorphism. Let σ be an element of $(A \otimes A)^*$ and set $R := \iota^{-1}(\sigma)$. Then*

(1) σ is convolution-invertible if and only if R is invertible as an element of the algebra $A^* \otimes A^*$.
(2) σ is a braiding of A if and only if R is a universal R -matrix of the dual Hopf algebra A^* .
In this case, the Drinfel'd element $\mu \in A^*$ of the quasitriangular Hopf algebra (A^*, R) is given by $\mu(a) = \sum \sigma(a_{(2)}, S(a_{(1)}))$ for all $a \in A$.

(3) for a finite-dimensional right A -comodule V , the equation $\underline{\dim}_R V = \underline{\dim}_\sigma V$ holds, where $\underline{\dim}_R V$ is the R -dimension of the left A^* -module V with the action

$$p \cdot v := \sum p(v_{(1)})v_{(0)} \quad (p \in A^*, v \in V).$$

Let C be a coalgebra over a field \mathbf{k} . A right C -comodule V is said to be an *absolutely simple* if the right C^K -comodule V^K is simple for an arbitrary field extension K/\mathbf{k} . This condition is equivalent to that V is absolutely simple as a left C^* -module. We note that if a right C -comodule is simple, then it is automatically finite-dimensional (see [19, Corollary 5.1.2]). So, there is a one-to-one correspondence between the absolutely simple right C -comodules and the absolutely simple left C^* -modules.

Let $\underline{\text{braid}}(A)$ denote the set of all braidings of a Hopf algebra A . Then by Part (2) of Lemma 4.3, the map

$$\underline{\text{braid}}(A) \longrightarrow \underline{\text{Braid}}(A^*), \quad \sigma \longmapsto \iota^{-1}(\sigma)$$

is bijective, and by Part (3) of the same lemma, the equation $\underline{\dim}_{\iota^{-1}(\sigma)} V = \underline{\dim}_\sigma V$ holds for a finite-dimensional right A -comodule V . Hence we have the following:

Lemma 4.4. *Let A be a semisimple and cosemisimple Hopf algebra over \mathbf{k} of finite dimension.*

(1) *For an absolutely simple right A -comodule V ,*

$$P_{A^*, V}(x) = \prod_{\sigma \in \underline{\text{braid}}(A)} \left(x - \frac{\underline{\dim}_\sigma V}{\dim V} \right),$$

where in the left-hand side $P_{A^*, V}(x)$ is the polynomial for V regarded as an left A^* -module by usual manner.

(2) *Let $\{V_1, \dots, V_t\}$ be a full set of non-isomorphic absolutely simple right A -comodules of dimension d . Then*

$$P_{A^*}^{(d)}(x) = \prod_{i=1}^t P_{A^*, V_i}(x).$$

A Hopf algebra A over a field \mathbf{k} of finite dimension is called *self-dual* if A is isomorphic to the dual Hopf algebra A^* as a Hopf algebra. Applying the above lemma to a self-dual Hopf algebra, we obtain immediately the following proposition.

Proposition 4.5. *Let A be a semisimple and cosemisimple Hopf algebra over a field \mathbf{k} of finite dimension. If A is self-dual, then for a positive integer d*

$$P_A^{(d)}(x) = \prod_{i=1}^t \prod_{\sigma \in \underline{\text{braid}}(A)} \left(x - \frac{\dim_{\sigma} V_i}{\dim V_i} \right),$$

where $\{V_1, \dots, V_t\}$ is a full set of non-isomorphic absolutely simple right A -comodules of dimension d .

By using the above formula, we compute the self-dual Hopf algebras $A_{Nn}^{+\lambda}$ introduced by Satoshi Suzuki [30] in the next section.

5 Examples

In this section we give several computational results of polynomial invariants of Hopf algebras. By comparing polynomial invariants one may find new examples of pairs of Hopf algebras such that their representation rings are isomorphic, but they are not monoidally Morita equivalent.

5.1 8-dimensional non-commutative semisimple Hopf algebras

By Masuoka [17], it is known that there are exactly three types of 8-dimensional non-commutative semisimple Hopf algebras over an algebraically closed field \mathbf{k} of $\text{ch}(\mathbf{k}) \neq 2$. They are $\mathbf{k}[D_8]$, $\mathbf{k}[Q_8]$ and K_8 , where D_8 and Q_8 are the dihedral group of order 8 and the quaternion group, respectively, and K_8 is the unique 8-dimensional semisimple Hopf algebra which is non-commutative and non-cocommutative, that is called the Kac-Paljutkin algebra [9]. Tambara and Yamagami [32] and also Masuoka [18] showed that their representation rings are isomorphic meanwhile their representation categories are not. In this subsection we derive this result by using our polynomial invariants. Throughout this subsection, we fix the following group presentations of D_8 and Q_8 :

$$\begin{aligned} D_8 &= \langle s, t \mid s^4 = 1, t^2 = 1, st = ts^{-1} \rangle, \\ Q_8 &= \langle s, t \mid s^4 = 1, t^2 = s^2, st = ts^{-1} \rangle. \end{aligned}$$

Let us start with determining the universal R -matrices of the group Hopf algebras $\mathbf{k}[D_8]$ and $\mathbf{k}[Q_8]$. For this the following proposition is useful.

Lemma 5.1. *Let G be a group, and \mathbf{k} a field. Then for a universal R -matrix R of $\mathbf{k}[G]$ there is a commutative and normal finite subgroup H such that $R \in \mathbf{k}[H] \otimes \mathbf{k}[H]$.*

Proof. We set $A = \mathbf{k}[G]$. By [25, Proposition 2(a)],

$$B = \{ (\text{id} \otimes \alpha)(R) \mid \alpha \in A^* \}, \quad H := \{ (\alpha \otimes \text{id})(R) \mid \alpha \in A^* \}$$

are finite-dimensional subHopf algebras of A . Since for each $g \in G$, $\mathbf{k}g$ is a subcoalgebra of $A = \bigoplus_{g \in G} \mathbf{k}g$, by [31, Lemma 9.0.1(b)] the subcoalgebra B is written in $B = \bigoplus_{g \in G} B \cap \mathbf{k}g$.

We set $K := B \cap G$. Then K is a subgroup of G , and $B \cap \mathbf{k}g \neq \{0\}$ if and only if $g \in K$. Thus $B = \bigoplus_{g \in K} B \cap \mathbf{k}g = \bigoplus_{g \in K} \mathbf{k}g = \mathbf{k}[K]$. Since B is finite-dimensional, K is a finite group. As a similar argument, we see that there is a finite subgroup L of G satisfying $H = \mathbf{k}[L]$. Since by [25, Proposition 2(c)] $\mathbf{k}[K]^{\text{cop}} \cong \mathbf{k}[L]$ as Hopf algebras, L is commutative. Furthermore, L is a normal subgroup of G since $Lg \subset gH$, or equivalently $g^{-1}Lg \subset H = \mathbf{k}[L]$ by [25, Proposition 3]. Similarly, we see that K is a commutative and normal subgroup of G .

At this point, $R \in \mathbf{k}[K] \otimes \mathbf{k}[L] \subset \mathbf{k}[LK] \otimes \mathbf{k}[LK]$ is verified. To complete the proof it is sufficient to show that LK is a commutative and normal subgroup of G . Since L is normal, it follows immediately that LK is normal. To show that LK is commutative, we write R in the form

$$R = \sum_{k \in K} k \otimes X_k \quad (X_k \in \mathbf{k}[L]).$$

Since $\Delta^{\text{cop}}(k') \cdot R = R \cdot \Delta(k')$ for all $k' \in K$, we have $X_{k'kk'^{-1}} = k'X_kk'^{-1}$ for all $k, k' \in K$. Since K is commutative, this condition is equivalent to $X_kk' = k'X_k$. It follows from $\mathbf{k}[L] = H = \text{Span}\{X_k \mid k \in K\}$ that any element $l \in L$ is represented by a \mathbf{k} -linear combination of $\{X_k \mid k \in K\}$. Thus $lk' = k'l$ holds. This means that LK is commutative. \square

For a cyclic group the universal R -matrices of the group Hopf algebra are given by (2.1) in Example 2.3 in Section 2. For a direct product of two cyclic groups the universal R -matrices of the group Hopf algebra are given as in the following lemma. The lemma can be verified by use of the same method of the proof of Lemma 5.15 described later.

Lemma 5.2. *Let G be the direct product of the cyclic groups $C_m = \langle g \rangle$ and $C_n = \langle h \rangle$, and let ω be a primitive mn -th root of unity in a field \mathbf{k} whose characteristic does not divide mn . We set $X(m, n) = \{d \in \{0, 1, \dots, m-1\} \mid dn \equiv 0 \pmod{m}\}$. Then any universal R -matrix of $\mathbf{k}[G]$ is given by the formula*

$$R_{pqrs}^{\mathbf{k}[G]} := \sum_{i,j=0}^{m-1} \sum_{k,l=0}^{n-1} \omega^{n(pij+rkj)+m(sk+l+qil)} E_{ik} \otimes E_{jl},$$

where $p \in X(m, m), q \in X(n, m), r \in X(m, n), s \in X(n, n)$, and $E_{ik} = \frac{1}{mn} \sum_{j=0}^{m-1} \sum_{l=0}^{n-1} \omega^{-nij-mkl} g^j h^l$.

By using Lemma 5.1 and Lemma 5.2, one can determine that the quasitriangular structures of $\mathbf{k}[D_8]$ and $\mathbf{k}[Q_8]$ as described in the following lemma [33].

Lemma 5.3. *Let \mathbf{k} be a field of $\text{ch}(\mathbf{k}) \neq 2$ that contains a primitive 4-th root of unity ζ .*

(1) *The quasitriangular structures of $\mathbf{k}[D_8]$ are given by*

(i) *universal R -matrices of $\mathbf{k}[\langle s \rangle] \cong \mathbf{k}[C_4]$:*

$$R_d^{\mathbf{k}[D_8]} := \frac{1}{4} \sum_{i,k=0}^3 \zeta^{-ik} s^k \otimes s^{di} \quad (d = 0, 1, 2, 3),$$

(ii) universal R -matrices of $\mathbf{k}[\langle t, s^2 \rangle] \cong \mathbf{k}[C_2 \times C_2]$:

$$R_{d+4}^{\mathbf{k}[D_8]} := \frac{1}{4} \sum_{i,j,k,l=0}^1 (-1)^{-ij-kl} t^i s^{2k} \otimes t^l s^{2(j+dl)} \quad (d = 0, 1),$$

(iii) universal R -matrices of $\mathbf{k}[\langle ts, s^2 \rangle] \cong \mathbf{k}[C_2 \times C_2]$:

$$R_{d+6}^{\mathbf{k}[D_8]} := \frac{1}{4} \sum_{i,j,k,l=0}^1 (-1)^{-ij-kl} (ts)^i s^{2k} \otimes (ts)^l s^{2(j+dl)} \quad (d = 0, 1).$$

The Drinfel'd element $u_d^{\mathbf{k}[D_8]}$ of $R_d^{\mathbf{k}[D_8]}$ is given by

$$u_d^{\mathbf{k}[D_8]} = \begin{cases} 1 & (d = 0, 4, 6), \\ \frac{1}{2}(1 + \zeta^{-1}) + \frac{1}{2}(1 + \zeta)s^2 & (d = 1), \\ s^2 & (d = 2, 5, 7), \\ \frac{1}{2}(1 + \zeta) + \frac{1}{2}(1 + \zeta^{-1})s^2 & (d = 3). \end{cases}$$

(2) The quasitriangular structures of $\mathbf{k}[Q_8]$ are given by

(i) universal R -matrices of $\mathbf{k}[\langle s \rangle] \cong \mathbf{k}[C_4]$:

$$R_d^{\mathbf{k}[Q_8]} := \frac{1}{4} \sum_{i,k=0}^3 \zeta^{-ik} s^k \otimes s^{di} \quad (d = 0, 1, 2, 3),$$

(ii) universal R -matrices of $\mathbf{k}[\langle t \rangle] \cong \mathbf{k}[C_4]$:

$$R_{d+4}^{\mathbf{k}[Q_8]} := \frac{1}{4} \sum_{i,k=0}^3 \zeta^{-ik} t^k \otimes t^{(2d+1)i} \quad (d = 0, 1),$$

(iii) universal R -matrices of $\mathbf{k}[\langle ts \rangle] \cong \mathbf{k}[C_4]$:

$$R_{d+6}^{\mathbf{k}[Q_8]} := \frac{1}{4} \sum_{i,k=0}^3 \zeta^{-ik} (ts)^k \otimes (ts)^{(2d+1)i} \quad (d = 0, 1).$$

The Drinfel'd element $u_d^{\mathbf{k}[Q_8]}$ of $R_d^{\mathbf{k}[Q_8]}$ is given by

$$u_d^{\mathbf{k}[Q_8]} = \begin{cases} 1 & (d = 0), \\ \frac{1}{2}(1 + \zeta^{-1}) + \frac{1}{2}(1 + \zeta)s^2 & (d = 1, 4, 6), \\ s^2 & (d = 2), \\ \frac{1}{2}(1 + \zeta) + \frac{1}{2}(1 + \zeta^{-1})s^2 & (d = 3, 5, 7). \end{cases}$$

Proof. In either case of $\mathbf{k}[D_8]$ or $\mathbf{k}[Q_8]$, the proof of the lemma can be done by the same method. So, we will determine the universal R -matrices only in the case of $\mathbf{k}[Q_8]$ (for $\mathbf{k}[D_8]$ see also Proposition 5.17 described later).

It is easy to show that the maximal commutative and normal subgroups of Q_8 coincide with one of $H_1 = \langle s \rangle$, $H_2 = \langle t \rangle$ and $H_3 = \langle ts \rangle$. Therefore, by Lemma 5.1 any universal R -matrix of $\mathbf{k}[Q_8]$ is that of $\mathbf{k}[H_i]$ for some $i = 1, 2, 3$. Let R be a universal R -matrix of $\mathbf{k}[H_1]$. Then $\Delta^{\text{cop}}(t) \cdot R = R \cdot \Delta(t)$ holds, and whence R is a universal R -matrix of $\mathbf{k}[Q_8]$. Similarly, we see that any universal R -matrix of $\mathbf{k}[H_i]$ for $i = 2, 3$ satisfies $\Delta^{\text{cop}}(s) \cdot R = R \cdot \Delta(s)$, and whence it is a universal R -matrix of $\mathbf{k}[Q_8]$. \square

Next, we describe the quasitriangular structures of the Kac-Paljutkin algebra K_8 , that are determined by S. Suzuki [30]. As an algebra the Kac-Paljutkin algebra K_8 coincides with the group algebra $\mathbf{k}[D_8]$. Let us consider the primitive orthogonal idempotents $e_0 = \frac{1+s^2}{2}$, $e_1 = \frac{1-s^2}{2}$ in $K_8 = \mathbf{k}[D_8]$. Then the Hopf algebra structure of K_8 is described as follows [18]:

$$\begin{aligned}\Delta(t) &= t \otimes e_0 t + st \otimes e_1 t, & \Delta(s) &= s \otimes e_0 s + s^{-1} \otimes e_1 s, \\ \varepsilon(t) &= 1, & \varepsilon(s) &= 1, \\ S(t) &= e_0 t + e_1 st, & S(s) &= e_0 s^{-1} + e_1 s.\end{aligned}$$

We note that $\Delta(e_0) = e_0 \otimes e_0 + e_1 \otimes e_1$, $\Delta(e_1) = e_0 \otimes e_1 + e_1 \otimes e_0$, $\varepsilon(e_0) = 1$, $\varepsilon(e_1) = 0$, $S(e_0) = e_0$, $S(e_1) = e_1$, and therefore, $\mathbf{k}e_0 + \mathbf{k}e_1$ is a subHopf algebra of K_8 which is isomorphic to the group Hopf algebra $\mathbf{k}[C_2]$. Let $\zeta \in \mathbf{k}$ be a primitive 4-th root of unity. Then

$$g := \frac{1}{2}(1 + \zeta)s + \frac{1}{2}(1 - \zeta)s^{-1}, \quad h := \frac{1}{2}(1 - \zeta)s + \frac{1}{2}(1 + \zeta)s^{-1}$$

satisfy $g^2 = h^2 = 1$, and $\mathbf{k}[\langle s \rangle] = \mathbf{k}1 + \mathbf{k}g + \mathbf{k}h + \mathbf{k}gh$ hold. Moreover, since g and h are group-like, the subHopf algebra $\mathbf{k}[\langle s \rangle]$ of K_8 is isomorphic to the group Hopf algebra $\mathbf{k}[C_2 \times C_2]$.

Lemma 5.4. *Let \mathbf{k} be a field of $\text{ch}(\mathbf{k}) \neq 2$ that contains a primitive 8-th root of unity ω . Then the universal R -matrices of K_8 are given as follows:*

(i) *universal R -matrices of $\mathbf{k}[\langle g, h \rangle] \cong \mathbf{k}[C_2 \times C_2]$:*

$$R_{pq}^{K_8} := \frac{1}{4} \sum_{i,j,k,l=0}^1 (-1)^{-(ij+kl)} g^i h^k \otimes g^{pj+(q+1)l} h^{qj+pl} \quad (p, q \in \{0, 1\}),$$

(ii) *minimal universal R -matrices of K_8 :*

$$R_l^{K_8} := \frac{1}{8} \sum_{i,j,p,q,r,s=0,1} \omega^{(2l+1)\frac{1-(-1)^i}{2} \cdot \frac{1-(-1)^j}{2}} (-1)^{jp+ir+(j(i+1)+l(j+r+s))(li+p+q)} t^i g^p h^q \otimes t^j g^r h^s$$

($l = 0, 1, 2, 3$).

The Drinfel'd elements $u_{p,q}^{K_8}$ and $u_l^{K_8}$ of $R_{p,q}^{K_8}$ and $R_l^{K_8}$, respectively, are given by

$$u_{pq}^{K_8} = \frac{1}{2} \sum_{i,l=0}^1 (-1)^{(i+p)(l+p)} g^i h^l \quad (p, q \in \{0, 1\}),$$

$$u_l^{K_8} = \frac{\omega^{2l-1}}{2} (1 - gh) + \frac{1}{2} (g + h) \quad (l = 0, 1, 2, 3).$$

Proof. Since the universal R -matrix $R_{pq}^{K_8}$ of $\mathbf{k}[\langle g, h \rangle]$ satisfies $\Delta^{\text{cop}}(t) \cdot R_{pq}^{K_8} = R_{pq}^{K_8} \cdot \Delta(t)$, we see immediately that $R_{pq}^{K_8}$ is a universal R -matrix of K_8 . It can be also verified straightforward that $R_l^{K_8}$ are indeed a universal R -matrix of K_8 , although the proof is tedious. Since K_8 is isomorphic to the Suzuki's Hopf algebra A_{12}^{+-} (for example see [2]), by [30, Proposition 3.10(ii)] the number of universal R -matrices of K_8 is 8. Thus there is no universal R -matrix of K_8 other than $R_{pq}^{K_8}$ ($p, q \in \{0, 1\}$) and $R_l^{K_8}$ ($l = 0, 1, 2, 3$). \square

Let \mathbf{k} be a field of $\text{ch}(\mathbf{k}) \neq 2$ that contains a primitive 4-th root of unity. Then for any of the algebras $\mathbf{k}[D_8]$, $\mathbf{k}[Q_8]$, K_8 the number of isomorphism classes of (absolutely) simple modules is 5. They consist of four 1-dimensional modules and one 2-dimensional simple module.

The 1-dimensional modules of $\mathbf{k}[D_8]$, $\mathbf{k}[Q_8]$ and K_8 are given by $V_{ij} = \mathbf{k}$ ($i, j = 0, 1$) equipped with the left actions ρ_{ij} defined by

$$\rho_{ij}(s) = (-1)^i, \quad \rho_{ij}(t) = (-1)^j.$$

For both $\mathbf{k}[D_8]$ and K_8 a 2-dimensional simple module, which is unique up to isomorphism, is given by $V = \mathbf{k} \oplus \mathbf{k}$ equipped with the left action ρ defined by

$$\rho(s) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \rho(t) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

and for $\mathbf{k}[Q_8]$ that is given by $V = \mathbf{k} \oplus \mathbf{k}$ equipped with the left action ρ defined by

$$\rho(s) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad \rho(t) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

where ζ is a primitive 4-th root of unity in \mathbf{k} .

Suppose that \mathbf{k} contains a primitive 8-th root of unity ω . Then by the above two lemmas we have $P_{\mathbf{k}[D_8], V_{ij}}(x) = P_{\mathbf{k}[Q_8], V_{ij}}(x) = (x - 1)^8$, $P_{K_8, V_{ij}}(x) = (x + (-1)^i)^8$ and

$$P_{\mathbf{k}[D_8], V}(x) = (x - 1)^3 (x + 1)^3 (x - \zeta)(x + \zeta) = x^8 - 2x^6 + 2x^2 - 1,$$

$$P_{\mathbf{k}[Q_8], V}(x) = (x - 1)(x + 1)(x - \zeta)^3 (x + \zeta)^3 = x^8 + 2x^6 - 2x^2 - 1,$$

$$P_{K_8, V}(x) = \prod_{p,q=0,1} (x - (-1)^p) \cdot \prod_{l=0}^3 (x - \omega^{2l-1}) = x^8 - 2x^6 + 2x^4 - 2x^2 + 1.$$

Therefore, the polynomial invariants of $\mathbf{k}[D_8]$, $\mathbf{k}[Q_8]$, K_8 are given by

$$P_{\mathbf{k}[D_8]}^{(1)}(x) = P_{\mathbf{k}[Q_8]}^{(1)}(x) = (x - 1)^{32}, \quad P_{K_8}^{(1)}(x) = (x - 1)^{16} (x + 1)^{16},$$

$$\begin{aligned}
P_{\mathbf{k}[D_8]}^{(2)}(x) &= x^8 - 2x^6 + 2x^2 - 1, \\
P_{\mathbf{k}[Q_8]}^{(2)}(x) &= x^8 + 2x^6 - 2x^2 - 1, \\
P_{K_8}^{(2)}(x) &= x^8 - 2x^6 + 2x^4 - 2x^2 + 1.
\end{aligned}$$

Since polynomials $P_{\mathbf{k}[D_8]}^{(2)}(x)$, $P_{\mathbf{k}[Q_8]}^{(2)}(x)$, $P_{K_8}^{(2)}(x)$ are mutually distinct, we conclude that the Hopf algebras $\mathbf{k}[D_8]$, $\mathbf{k}[Q_8]$, K_8 are not mutually monoidally Morita equivalent by Theorem 2.6.

5.2 The Hopf algebra $A_{Nn}^{\nu\lambda}$

Satoshi Suzuki introduced a family of cosemisimple Hopf algebras of finite dimension parametrized by ν, λ, N, n , where $\nu, \lambda = \pm 1$, and $N \geq 1$ and $n \geq 2$ are integers. This family includes not only the Kac-Paljutkin algebra K_8 , but also Hopf algebras which can be regarded as a generalization of K_8 . In this subsection we compute the polynomial invariants for Suzuki's Hopf algebras.

Let us recall the definition of Suzuki's Hopf algebras $A_{Nn}^{\nu\lambda}$ [30]. Let \mathbf{k} be a field of $\text{ch}(\mathbf{k}) \neq 2$, which contains a primitive $4nN$ -th root of unity, and let C be the 2×2 -matrix coalgebra over \mathbf{k} . By definition C has a basis $\{X_{11}, X_{12}, X_{21}, X_{22}\}$ which satisfies the equation

$$\Delta(X_{ij}) = X_{i1} \otimes X_{1j} + X_{i2} \otimes X_{2j}, \quad \varepsilon(X_{ij}) = \delta_{ij}.$$

Since C is a coalgebra, the tensor algebra $\mathcal{T}(C)$ of C has a bialgebra structure in a natural way. Let I be the coideal of $\mathcal{T}(C)$ defined by

$$I = \mathbf{k}(X_{11}^2 - X_{22}^2) + \mathbf{k}(X_{12}^2 - X_{21}^2) + \sum_{i-j \not\equiv l-m \pmod{2}} \mathbf{k}(X_{ij}X_{lm}),$$

and consider the quotient bialgebra $B := \mathcal{T}(C)/\langle I \rangle$. We write x_{ij} for the image of X_{ij} under the natural projection $\mathcal{T}(C) \longrightarrow B$. We fix $N \geq 1$, $n \geq 2$ and $\nu, \lambda = \pm 1$, and consider the following subspace $J_{Nn}^{\nu\lambda}$ of B :

$$\begin{aligned}
J_{Nn}^{\nu\lambda} := & \mathbf{k}(x_{11}^{2N} + \nu x_{12}^{2N} - 1) \\
& + \mathbf{k}(\underbrace{x_{11}x_{22}x_{11} \cdots}_{n} - \underbrace{x_{22}x_{11}x_{22} \cdots}_{n}) + \mathbf{k}(-\lambda \underbrace{x_{12}x_{21}x_{12} \cdots}_{n} + \underbrace{x_{21}x_{12}x_{21} \cdots}_{n}).
\end{aligned}$$

Here,

$$\underbrace{x_{11}x_{22}x_{11} \cdots}_{n} = \begin{cases} (x_{11}x_{22})^{\frac{n}{2}} & \text{if } n \text{ is even,} \\ (x_{11}x_{22})^{\frac{n-1}{2}} x_{11} & \text{if } n \text{ is odd,} \end{cases}$$

and the other notation has the same meaning of that, too. Since the subspace $J_{Nn}^{\nu\lambda}$ is a coideal of B , we obtain the quotient bialgebra $A_{Nn}^{\nu\lambda} := B/\langle J_{Nn}^{\nu\lambda} \rangle$. This bialgebra $A_{Nn}^{\nu\lambda}$ becomes a $4nN$ -dimensional cosemisimple Hopf algebra over \mathbf{k} . For the image of x_{ij} under the natural projection $\pi : B \longrightarrow A_{Nn}^{\nu\lambda}$ we write x_{ij} , again. Then $A_{Nn}^{\nu\lambda}$ equips with the basis

$$\{x_{11}^s \underbrace{x_{22}x_{11}x_{22} \cdots}_{t}, x_{12}^s \underbrace{x_{21}x_{12}x_{21} \cdots}_{t} \mid 1 \leq s \leq 2N, 0 \leq t \leq n-1\}, \quad (5.1)$$

and the Hopf algebra structure is given by

$$\Delta(x_{ij}) = x_{i1} \otimes x_{1j} + x_{i2} \otimes x_{2j}, \quad \varepsilon(x_{ij}) = \delta_{ij}, \quad S(x_{ij}) = x_{ji}^{2N-1}.$$

If $\text{ch}(\mathbf{k}) \nmid 2nN$, then $A_{Nn}^{\nu\lambda}$ is semisimple [30, Theorem 3.1(viii)]. Moreover, A_{12}^{+-} is isomorphic to the Kac-Paljutkin algebra K_8 , and the Hopf algebras A_{1n}^{++} and A_{1n}^{+-} are isomorphic to the Hopf algebras \mathcal{A}_{4n} and \mathcal{B}_{4n} , respectively, that are introduced by Masuoka [18, 2]. The following lemma, which is a direct consequence of the definition of $A_{Nn}^{\nu\lambda}$, is useful for computation.

Lemma 5.5. *For each $i, j = 1, 2$, the square x_{ij}^2 is in the center of $A_{Nn}^{\nu\lambda}$, and the following equations hold in $A_{Nn}^{\nu\lambda}$.*

- (1) $x_{11}^2 = x_{22}^2$, $x_{12}^2 = x_{21}^2$, $x_{ij}x_{lm} = 0$ ($i - j \not\equiv l - m \pmod{2}$).
- (2) If n is even, then $(x_{22}x_{11})^{\frac{n}{2}} = (x_{11}x_{22})^{\frac{n}{2}}$, $(x_{21}x_{12})^{\frac{n}{2}} = \lambda(x_{12}x_{21})^{\frac{n}{2}}$.
If n is odd, then $(x_{22}x_{11})^{\frac{n-1}{2}}x_{22} = (x_{11}x_{22})^{\frac{n-1}{2}}x_{11}$, $(x_{21}x_{12})^{\frac{n-1}{2}}x_{21} = \lambda(x_{12}x_{21})^{\frac{n-1}{2}}x_{12}$.
- (3) $x_{ii}^{2N+1} = x_{ii}$, $x_{i\ i+1}^{2N+1} = \nu x_{i\ i+1}$.
- (4) $x_{11}^{4N} + x_{12}^{4N} = 1$.
- (5) $(x_{11}x_{22})^n = x_{11}^{2n}$, $(x_{21}x_{12})^n = \lambda x_{12}^{2n}$.

To describe the simple right $A_{Nn}^{\nu\lambda}$ -comodules, we use the following notations. For $m \geq 1$, we set

$$\begin{aligned} \chi_{11}^m &:= \overbrace{x_{11}x_{22}x_{11} \dots}^m, \quad \chi_{22}^m := \overbrace{x_{22}x_{11}x_{22} \dots}^m, \\ \chi_{12}^m &:= \overbrace{x_{12}x_{21}x_{12} \dots}^m, \quad \chi_{21}^m := \overbrace{x_{21}x_{12}x_{21} \dots}^m. \end{aligned}$$

Then the basis (5.1) of $A_{Nn}^{\nu\lambda}$ can be represented by

$$\{ x_{11}^s \chi_{22}^t, x_{12}^s \chi_{21}^t \mid 1 \leq s \leq 2N, 0 \leq t \leq n-1 \}, \quad (5.2)$$

and the following equations hold:

$$\Delta(\chi_{ij}^m) = \chi_{i1}^m \otimes \chi_{1j}^m + \chi_{i2}^m \otimes \chi_{2j}^m \quad (m \geq 1, i, j = 1, 2). \quad (5.3)$$

Thus for $s, t \geq 0$ with $s + t \geq 1$,

$$\begin{aligned} \Delta(x_{11}^s \chi_{22}^t) &= x_{11}^s \chi_{22}^t \otimes x_{11}^s \chi_{22}^t + x_{12}^s \chi_{21}^t \otimes x_{21}^s \chi_{12}^t, \\ \Delta(x_{12}^s \chi_{21}^t) &= x_{11}^s \chi_{22}^t \otimes x_{12}^s \chi_{21}^t + x_{12}^s \chi_{21}^t \otimes x_{22}^s \chi_{11}^t. \end{aligned}$$

Furthermore,

$$S(x_{11}^s \chi_{22}^t) = \begin{cases} x_{11}^{(2N-2)(t+s)+s} \chi_{11}^t & (s, t \text{ are even}), \\ x_{11}^{(2N-2)(t+s)+s} \chi_{22}^t & (s \text{ is odd, and } t \text{ is even}), \\ x_{11}^{(2N-2)(t+s)+s} \chi_{22}^t & (s \text{ is even, and } t \text{ is odd}), \\ x_{22}^{(2N-2)(t+s)+s} \chi_{11}^t & (s, t \text{ are odd}), \end{cases}$$

$$S(x_{12}^s \chi_{21}^t) = \begin{cases} x_{12}^{(2N-2)(t+s)+s} \chi_{21}^t & (s, t \text{ are even}), \\ x_{21}^{(2N-2)(t+s)+s} \chi_{12}^t & (s \text{ is odd, and } t \text{ is even}), \\ x_{12}^{(2N-2)(t+s)+s} \chi_{12}^t & (s \text{ is even, and } t \text{ is odd}), \\ x_{12}^{(2N-2)(t+s)+s} \chi_{21}^t & (s, t \text{ are odd}). \end{cases}$$

Hereafter to the end of this subsection we suppose that $N \geq 1$, $n \geq 2$ and $\nu, \lambda = \pm 1$, and \mathbf{k} is a field of $\text{ch}(\mathbf{k}) \neq 2$, which contains a primitive $4nN$ -th root of unity. The following proposition was proved by S. Suzuki.

Proposition 5.6 ([30, Theorem 3.1]).

- (1) The dimension of a simple subcoalgebra of $A_{Nn}^{\nu\lambda}$ is 1 or 4.
- (2) The order of the group $G := G(A_{Nn}^{\nu\lambda})$ is $4N$, and G is explicitly given by

$$G = \{ x_{11}^{2s} \pm x_{12}^{2s}, x_{11}^{2s+1} \chi_{22}^{n-1} \pm \sqrt{\lambda} x_{12}^{2s+1} \chi_{21}^{n-1} \mid 1 \leq s \leq N \}.$$

- (3) There are exactly $N(n-1)$ simple subcoalgebras of dimension 4, and they are given by

$$C_{st} = \mathbf{k} x_{11}^{2s} \chi_{11}^t + \mathbf{k} x_{12}^{2s} \chi_{12}^t + \mathbf{k} x_{12}^{2s} \chi_{21}^t + \mathbf{k} x_{11}^{2s} \chi_{22}^t \quad (0 \leq s \leq N-1, 1 \leq t \leq n-1).$$

Therefore, the cosemisimple Hopf algebra $A_{Nn}^{\nu\lambda}$ is decomposed to the direct sum of simple subcoalgebras such as

$$A_{Nn}^{\nu\lambda} = \bigoplus_{g \in G} \mathbf{k}g \oplus \bigoplus_{\substack{0 \leq s \leq N-1 \\ 1 \leq t \leq n-1}} C_{st}.$$

Corollary 5.7. The set

$$\{ \mathbf{k}g \mid g \in G(A_{Nn}^{\nu\lambda}) \} \cup \{ \mathbf{k} x_{11}^{2s} \chi_{22}^t + \mathbf{k} x_{12}^{2s} \chi_{21}^t \mid 0 \leq s \leq N-1, 1 \leq t \leq n-1 \}$$

is a full set of non-isomorphic (absolutely) simple right $A_{Nn}^{\nu\lambda}$ -comodules, where the coactions of the comodules listed above are given by restrictions of the coproduct Δ .

Proof. Since $A_{Nn}^{\nu\lambda}$ is cosemisimple, a full set of non-isomorphic simple right $A_{Nn}^{\nu\lambda}$ -comodules can be obtained by taking a simple right D -comodule for each simple subcoalgebra D of $A_{Nn}^{\nu\lambda}$ and by collecting them.

Let D be a simple subcoalgebra of $A_{Nn}^{\nu\lambda}$. If $\dim D = 1$, then $D = \mathbf{k}g$ for some $g \in G(A_{Nn}^{\nu\lambda})$. So, we can take D itself as a simple right D -comodule. If $\dim D = 4$, then by Proposition 5.6 (3), $D = C_{st}$ for some $s \in \{0, 1, \dots, N-1\}$ and $t \in \{1, \dots, n-1\}$. Let us consider the subspace

$$V_{st} := \mathbf{k} x_{11}^{2s} \chi_{22}^t + \mathbf{k} x_{12}^{2s} \chi_{21}^t$$

of D . Then the subspace V_{st} is a right D -comodule. For

$$\begin{aligned} \Delta(x_{11}^{2s} \chi_{22}^t) &= x_{11}^{2s} \chi_{22}^t \otimes x_{11}^{2s} \chi_{22}^t + x_{12}^{2s} \chi_{21}^t \otimes x_{21}^{2s} \chi_{12}^t, \\ \Delta(x_{12}^{2s} \chi_{21}^t) &= x_{11}^{2s} \chi_{22}^t \otimes x_{12}^{2s} \chi_{21}^t + x_{12}^{2s} \chi_{21}^t \otimes x_{22}^{2s} \chi_{11}^t, \end{aligned}$$

and $x_{21}^{2s} \chi_{12}^t = x_{12}^{2s} \chi_{12}^t$, $x_{22}^{2s} \chi_{11}^t = x_{11}^{2s} \chi_{11}^t \in C_{st}$. Furthermore, the right D -comodule V_{st} is simple, since there is no non-zero element $v \in V_{st}$ such that $\Delta(v) \in \mathbf{k}v \otimes C_{st}$. \square

Let us explain on the braiding structures of $A_{Nn}^{\nu\lambda}$, which is determined by S. Suzuki [30]. Suppose that $\alpha, \beta \in \mathbf{k}$ satisfy $(\alpha\beta)^N = \nu$, $(\alpha\beta^{-1})^n = \lambda$. Then there is a braiding $\sigma_{\alpha\beta}$ of $A_{Nn}^{\nu\lambda}$ such that the values $\sigma_{\alpha\beta}(x_{ij}, x_{kl})$ ($i, j, k, l = 1, 2$) are given by the list below.

$x \setminus y$	x_{11}	x_{12}	x_{21}	x_{22}
x_{11}	0	0	0	0
x_{12}	0	α	β	0
x_{21}	0	β	α	0
x_{22}	0	0	0	0

In fact, by using the braiding conditions (B2) and (B3) described in Section 4, repeatedly, we see that the values of $\sigma_{\alpha\beta}$ on the basis (5.2) are given as follows: for integers $s, s', t, t' \geq 0$ with $s + t \geq 1$ and $s' + t' \geq 1$, and $j' = 1, 2$,

$$\begin{aligned}
& \sigma_{\alpha\beta}(x_{11}^s \chi_{22}^t, x_{1j'}^{s'} \chi_{2,j'+1}^{t'}) \\
&= \begin{cases} \delta_{0,t'} \delta_{1+j',t} (\alpha\beta)^{\frac{t's+(s+t)s'}{2}} \beta^{tt'} & (s \text{ and } s' \text{ are even}), \\ \delta_{1,t'} \delta_{1+j',t} (\alpha\beta)^{\frac{t's+(s+t)s'-t}{2}} \alpha^{t(t'+1)} & (s \text{ is even, and } s' \text{ is odd}), \\ \delta_{0,t'} \delta_{j',t} (\alpha\beta)^{\frac{t's+(s+t)s'-t'}{2}} \alpha^{(t+1)t'} & (s \text{ is odd, and } s' \text{ is even}), \\ \delta_{1,t'} \delta_{j',t} (\alpha\beta)^{\frac{t's+(s+t)s'-(1+t+t')}{2}} \beta^{(t+1)(t'+1)} & (s \text{ and } s' \text{ are odd}), \end{cases} \\
& \sigma_{\alpha\beta}(x_{12}^s \chi_{21}^t, x_{1j'}^{s'} \chi_{2,j'+1}^{t'}) \\
&= \begin{cases} \delta_{1,t'} \delta_{1+j',t} (\alpha\beta)^{\frac{t's+(s+t)s'}{2}} \alpha^{tt'} & (s \text{ and } s' \text{ are even}), \\ \delta_{0,t'} \delta_{1+j',t} (\alpha\beta)^{\frac{t's+(s+t)s'-t}{2}} \beta^{t(t'+1)} & (s \text{ is even, and } s' \text{ is odd}), \\ \delta_{1,t'} \delta_{j',t} (\alpha\beta)^{\frac{t's+(s+t)s'-t'}{2}} \beta^{(t+1)t'} & (s \text{ is odd, and } s' \text{ is even}), \\ \delta_{0,t'} \delta_{j',t} (\alpha\beta)^{\frac{t's+(s+t)s'-(1+t+t')}{2}} \alpha^{(t+1)(t'+1)} & (s \text{ and } s' \text{ are odd}), \end{cases}
\end{aligned}$$

where the indices of χ and δ are treated as modulo 2.

When $n = 2$, in addition to the above braidings $\sigma_{\alpha\beta}$, for $\gamma, \xi \in \mathbf{k}$ which satisfy $\gamma^2 = \xi^2$, $\gamma^{2N} = 1$ there is a braiding $\tau_{\gamma\xi}$ of $A_{N2}^{\nu\lambda}$ such that the values $\tau_{\gamma\xi}(x_{ij}, x_{kl})$ ($i, j, k, l = 1, 2$) are given by the list below, where x_{ij} and x_{kl} correspond to a row and a column, respectively.

$x \setminus y$	x_{11}	x_{12}	x_{21}	x_{22}
x_{11}	γ	0	0	ξ
x_{12}	0	0	0	0
x_{21}	0	0	0	0
x_{22}	$\lambda\xi$	0	0	γ

We see also that the values of $\tau_{\gamma\xi}$ on the basis (5.2) are given as follows: for integers

$s, s', t, t' \geq 0$ with $s + t \geq 1$ and $s' + t' \geq 1$, and $j' = 1, 2$,

$$\begin{aligned} & \tau_{\gamma\xi}(x_{11}^s \chi_{22}^t, x_{1j'}^{s'} \chi_{2,j'+1}^{t'}) \\ &= \begin{cases} \delta_{j'1} \gamma^{ss'} (\gamma\xi)^{\frac{tt'}{4} + \frac{st'}{2}} (\gamma\lambda\xi)^{\frac{tt'}{4} + \frac{ts'}{2}} & (t \text{ and } t' \text{ are even}), \\ \delta_{j'1} \gamma^{ss'} (\lambda\xi)^{s'} (\gamma\xi)^{\frac{(t-1)t'}{4} + \frac{st'}{2}} (\gamma\lambda\xi)^{\frac{(t+1)t'}{4} + \frac{(t-1)s'}{2}} & (t \text{ is odd, and } t' \text{ is even}), \\ \delta_{j'1} \gamma^{ss'} \xi^s (\gamma\xi)^{\frac{t(t'+1)}{4} + \frac{s(t'-1)}{2}} (\gamma\lambda\xi)^{\frac{t(t'-1)}{4} + \frac{ts'}{2}} & (t \text{ is even, and } t' \text{ is odd}), \\ \delta_{j'1} \gamma^{ss'+1} \xi^s (\lambda\xi)^{s'} (\gamma\xi)^{\frac{(t-1)(t'+1)}{4} + \frac{s(t'-1)}{2}} (\gamma\lambda\xi)^{\frac{(t+1)(t'-1)}{4} + \frac{(t-1)s'}{2}} & (t \text{ and } t' \text{ are odd}), \end{cases} \\ & \tau_{\gamma\xi}(x_{12}^s \chi_{21}^t, x_{1j'}^{s'} \chi_{2,j'+1}^{t'}) = 0, \end{aligned}$$

where the indices of χ and δ are treated as modulo 2.

Theorem 5.8 ([30, Proposition 3.10]). *If $n \geq 3$, then the braidings of $A_{Nn}^{\nu\lambda}$ are given by*

$$\{ \sigma_{\alpha\beta} \mid \alpha, \beta \in \mathbf{k}, (\alpha\beta)^N = \nu, (\alpha\beta^{-1})^n = \lambda \},$$

and if $n = 2$, then that are given by

$$\{ \sigma_{\alpha\beta} \mid \alpha, \beta \in \mathbf{k}, (\alpha\beta)^N = \nu, (\alpha\beta^{-1})^2 = \lambda \} \cup \{ \tau_{\gamma\xi} \mid \gamma, \xi \in \mathbf{k}, \gamma^2 = \xi^2, \gamma^{2N} = 1 \}.$$

Lemma 5.9. (1) *For $\alpha, \beta \in \mathbf{k}$ satisfying $(\alpha\beta)^N = \nu$, $(\alpha\beta^{-1})^n = \lambda$, the Drinfel'd element $\mu_{\alpha\beta}$ of the braided Hopf algebra $(A_{Nn}^{\nu\lambda}, \sigma_{\alpha\beta})$ is given as follows: for all integers $s, t \geq 0$ with $s + t \geq 1$,*

$$\begin{aligned} \mu_{\alpha\beta}(x_{11}^s \chi_{22}^t) &= \begin{cases} \nu^t (\alpha\beta)^{\frac{-s^2}{2} - st - t^2} \alpha^{t^2} & (s \text{ is even}), \\ \nu^{t+1} (\alpha\beta)^{\frac{-1-s^2}{2} - t - st - t^2} \alpha^{(t+1)^2} & (s \text{ is odd}), \end{cases} \\ \mu_{\alpha\beta}(x_{12}^s \chi_{21}^t) &= 0. \end{aligned}$$

(2) *For $\gamma, \xi \in \mathbf{k}$ satisfying $\gamma^2 = \xi^2$, $\gamma^{2N} = 1$, the Drinfel'd element $\mu_{\gamma\xi}$ of the braided Hopf algebra $(A_{N2}^{\nu\lambda}, \tau_{\gamma\xi})$ is given as follows: for all integers $s, t \geq 0$ with $s + t \geq 1$,*

$$\begin{aligned} \mu_{\gamma\xi}(x_{11}^s \chi_{22}^t) &= \begin{cases} \gamma^{-s^2 - 2st - t^2} \lambda^{\frac{t^2}{4}} & (s \text{ and } t \text{ are even}), \\ \gamma^{-s^2 - 2st - t^2} \lambda^{\frac{t^2 - 1}{4}} & (t \text{ is odd, and } s \text{ is even}), \\ \gamma^{-s^2 - 2st - t^2} \lambda^{\frac{t(t+2)}{4}} & (t \text{ is even, and } s \text{ is odd}), \\ \gamma^{-s^2 - 2st - t^2} \lambda^{\frac{(t+1)^2}{4}} & (s \text{ and } t \text{ are odd}), \end{cases} \\ \mu_{\gamma\xi}(x_{12}^s \chi_{21}^t) &= 0. \end{aligned}$$

Proof. In the case where s and t are even, and $t \geq 2$, the values $\mu_{\alpha\beta}(a)$ and $\mu_{\gamma\xi}(a)$ for $a = x_{11}^s \chi_{22}^t$, $x_{12}^s \chi_{21}^t$ can be calculated as follows.

$$\begin{aligned} \mu_{\alpha\beta}(x_{11}^s \chi_{22}^t) &= \sigma_{\alpha\beta}(x_{11}^s \chi_{22}^t, x_{11}^{(2N-2)(s+t)+s+1} \chi_{22}^{t-1}) + \sigma_{\alpha\beta}(x_{12}^{s+1} \chi_{21}^{t-1}, x_{12}^{(2N-2)(s+t)+s} \chi_{21}^t) \\ &= (\alpha\beta)^{\frac{(t-1)s + (s+t)((2N-2)(s+t)+s+1)-t}{2}} \alpha^{t^2} \\ &= (\alpha\beta)^{(s+t)^2 N} (\alpha\beta)^{-\frac{s^2}{2} - st - t^2} \alpha^{t^2} \\ &= (\alpha\beta)^{-\frac{s^2}{2} - st - t^2} \alpha^{t^2}, \end{aligned}$$

$$\begin{aligned}
\mu_{\alpha\beta}(x_{12}^s \chi_{21}^t) &= \sigma_{\alpha\beta}(x_{12}^s \chi_{21}^t, x_{11}^{(2N-2)(s+t)+s+1} \chi_{22}^{t-1}) + \sigma_{\alpha\beta}(x_{11}^{s+1} \chi_{22}^{t-1}, x_{12}^{(2N-2)(s+t)+s} \chi_{21}^t) \\
&= 0, \\
\mu_{\gamma\xi}(x_{11}^s \chi_{22}^t) &= \tau_{\gamma\xi}(x_{11}^s \chi_{22}^t, x_{11}^{(2N-2)(s+t)+s+1} \chi_{22}^{t-1}) + \tau_{\gamma\xi}(x_{12}^{s+1} \chi_{21}^{t-1}, x_{12}^{(2N-2)(s+t)+s} \chi_{21}^t) \\
&= \gamma^{s((2N-2)(s+t)+s+1)} \xi^s (\gamma\xi)^{\frac{t^2}{4} + \frac{s(t-2)}{2}} (\gamma\lambda\xi)^{\frac{t(t-2)}{4} + \frac{t((2N-2)(s+t)+s+1)}{2}} \\
&= \gamma^{-2(s+t)^2+s^2+ts+\frac{t(t+s)}{2}} \xi^{\frac{t(t+s)}{2}} \lambda^{\frac{t^2}{4}} \\
&= \gamma^{(s+t)(-s-t)} \lambda^{\frac{t^2}{4}}, \\
\mu_{\gamma\xi}(x_{12}^s \chi_{21}^t) &= \tau_{\gamma\xi}(x_{12}^s \chi_{21}^t, x_{11}^{(2N-2)(s+t)+s+1} \chi_{22}^{t-1}) + \tau_{\gamma\xi}(x_{11}^{s+1} \chi_{22}^{t-1}, x_{12}^{(2N-2)(s+t)+s} \chi_{21}^t) \\
&= 0.
\end{aligned}$$

In other cases, the values $\mu_{\alpha\beta}(a)$ and $\mu_{\gamma\xi}(a)$ for $a = x_{11}^s \chi_{22}^t, x_{12}^s \chi_{21}^t$ can be calculated by a similar manner, so we leave the rest of calculation to the reader. \square

By using Lemma 5.9, we know the braided dimensions of the simple right $A_{Nn}^{\nu\lambda}$ -comodules.

Lemma 5.10. (1) Let α, β be elements in \mathbf{k} satisfying $(\alpha\beta)^N = \nu$ and $(\alpha\beta^{-1})^n = \lambda$.

(i) For an element $g \in G(A_{Nn}^{\nu\lambda})$ the character $\chi_g \in A_{Nn}^{\nu\lambda}$ of the simple right $A_{Nn}^{\nu\lambda}$ -comodule $\mathbf{k}g$ is given by $\chi_g = g$, and the braided dimension $\underline{\dim}_{\sigma_{\alpha\beta}} \mathbf{k}g$ with respect to the braiding $\sigma_{\alpha\beta}$ is given by

$$\underline{\dim}_{\sigma_{\alpha\beta}} \mathbf{k}g = \begin{cases} (\alpha\beta)^{-2s^2} & (g = x_{11}^{2s} \pm x_{12}^{2s} \ (1 \leq s \leq N)), \\ \nu^n (\alpha\beta)^{-2s^2-2sn-n^2} \alpha^{n^2} & (g = x_{11}^{2s+1} \chi_{22}^{n-1} \pm \sqrt{\lambda} x_{12}^{2s+1} \chi_{21}^{n-1} \ (1 \leq s \leq N)). \end{cases}$$

(ii) For the simple right $A_{Nn}^{\nu\lambda}$ -comodule $V_{st} = \mathbf{k}x_{11}^{2s} \chi_{22}^t + \mathbf{k}x_{12}^{2s} \chi_{21}^t$ ($0 \leq s \leq N-1, 1 \leq t \leq n-1$), the character $\chi_{st} \in A_{Nn}^{\nu\lambda}$ of V_{st} is given by $\chi_{st} = x_{11}^{2s+1} \chi_{22}^{t-1} + x_{11}^{2s} \chi_{22}^t$, and the braided dimension $\underline{\dim}_{\sigma_{\alpha\beta}} V_{st}$ is given by

$$\underline{\dim}_{\sigma_{\alpha\beta}} V_{st} = 2\nu^t \alpha^{t^2} (\alpha\beta)^{-2s^2-2st-t^2}.$$

(2) Let γ, ξ be elements in \mathbf{k} such that $\gamma^2 = \xi^2, \gamma^{2N} = 1$.

(i) For an element $g \in G(A_{N2}^{\nu\lambda})$ the braided dimension $\underline{\dim}_{\tau_{\gamma\xi}} \mathbf{k}g$ is given by

$$\underline{\dim}_{\tau_{\gamma\xi}} \mathbf{k}g = \begin{cases} \gamma^{-4s^2} & (g = x_{11}^{2s} \pm x_{12}^{2s} \ (1 \leq s \leq N)), \\ \gamma^{-4(s+1)^2} \lambda & (g = x_{11}^{2s+1} \chi_{22} \pm \sqrt{\lambda} x_{12}^{2s+1} \chi_{21} \ (1 \leq s \leq N)). \end{cases}$$

(ii) For the simple right $A_{N2}^{\nu\lambda}$ -comodule $V_{s1} = \mathbf{k}x_{11}^{2s} x_{22} + \mathbf{k}x_{12}^{2s} x_{21}$ ($0 \leq s \leq N-1$), the braided dimension $\underline{\dim}_{\tau_{\gamma\xi}} V_{s1}$ is given by

$$\underline{\dim}_{\tau_{\gamma\xi}} V_{s1} = 2\gamma^{-(2s+1)^2}.$$

Proposition 5.11. *Let $\omega \in \mathbf{k}$ be a primitive $4nN$ -th root of unity.*

(1) *For each $g \in G(A_{Nn}^{\nu\lambda})$, the polynomial $P_{(A_{Nn}^{\nu\lambda})^*, \mathbf{k}g}(x)$ is given as follows. If $g = x_{11}^{2s} \pm x_{12}^{2s}$ ($1 \leq s \leq N$), then*

$$P_{(A_{Nn}^{\nu\lambda})^*, \mathbf{k}g}(x) = \begin{cases} \prod_{i=0}^{N-1} (x - \omega^{-4n(2i+\frac{1-\nu}{2})s^2})^{2n} & (n \geq 3), \\ \prod_{i=0}^{N-1} (x - \omega^{-8(2i+\frac{1-\nu}{2})s^2})^4 (x - \omega^{-16is^2})^4 & (n = 2), \end{cases}$$

and if $g = x_{11}^{2s+1} \chi_{22}^{n-1} \pm \sqrt{\lambda} x_{12}^{2s+1} \chi_{21}^{n-1}$ ($1 \leq s \leq N$), then

$$P_{(A_{Nn}^{\nu\lambda})^*, \mathbf{k}g}(x) = \begin{cases} \prod_{i=0}^{N-1} (x^2 - \omega^{-2n(2s+n)^2(2i+\frac{1-\nu}{2})} (-1)^{\frac{1-\lambda}{2}})^n & (n \text{ is odd}), \\ \prod_{i=0}^{N-1} (x - \omega^{-n(2s+n)^2(2i+\frac{1-\nu}{2})} (-1)^{\frac{n}{2}\frac{1-\lambda}{2}})^{2n} & (n \geq 4 \text{ is even}), \\ \prod_{i=0}^{N-1} (x - \omega^{-4(s+1)^2(2i+\frac{1-\nu}{2})} (-1)^{\frac{1-\lambda}{2}})^4 (x - \omega^{-16i(s+1)^2} \lambda)^4 & (n = 2). \end{cases}$$

(2) *For the simple right $A_{Nn}^{\nu\lambda}$ -comodule $V_{st} = \mathbf{k}x_{11}^{2s}\chi_{22}^t + \mathbf{k}x_{12}^{2s}\chi_{21}^t$ ($0 \leq s \leq N-1$, $1 \leq t \leq n-1$), the polynomial $P_{(A_{Nn}^{\nu\lambda})^*, V_{st}}(x)$ is given by*

$$P_{(A_{Nn}^{\nu\lambda})^*, V_{st}}(x) = \begin{cases} \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x^2 - \omega^{-2n(2s+t)^2(2i+\frac{1-\nu}{2})-2Nt^2(2j+\frac{\lambda-1}{2})}) & (n \geq 3, \text{ and } t \text{ is odd}), \\ \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - \omega^{-n(2s+t)^2(2i+\frac{1-\nu}{2})-Nt^2(2j+\frac{\lambda-1}{2})})^2 & (n \geq 3, \text{ and } t \text{ is even}), \\ \prod_{i=0}^{N-1} (x^4 - \omega^{-8(2i+\frac{1-\nu}{2})(2s+1)^2+2N(1-\lambda)}) (x^2 - \omega^{-8i(2s+1)^2})^2 & (n = 2). \end{cases}$$

Proof. The set $I_{\nu\lambda} = \{ (\alpha, \beta) \in \mathbf{k} \times \mathbf{k} \mid (\alpha\beta)^N = \nu, (\alpha\beta^{-1})^n = \lambda \}$ can be expressed as

$$I_{\nu\lambda} = \left\{ \left(\omega^{n(2i+\frac{1-\nu}{2})+N(2j+\frac{1-\lambda}{2})}, \omega^{n(2i+\frac{1-\nu}{2})-N(2j+\frac{1-\lambda}{2})} \right) \mid \begin{array}{l} i = 0, 1, \dots, N-1, \\ j = 0, 1, \dots, n-1 \end{array} \right\} \\ \cup \left\{ \left(-\omega^{n(2i+\frac{1-\nu}{2})+N(2j+\frac{1-\lambda}{2})}, -\omega^{n(2i+\frac{1-\nu}{2})-N(2j+\frac{1-\lambda}{2})} \right) \mid \begin{array}{l} i = 0, 1, \dots, N-1, \\ j = 0, 1, \dots, n-1 \end{array} \right\}.$$

Because, for an element $(\alpha, \beta) \in I_{\nu\lambda}$, $\alpha\beta$ and $\alpha\beta^{-1}$ can be written as

$$\begin{cases} \alpha\beta = \omega^{2n(2i+\frac{1-\nu}{2})} & \text{for some } i = 0, 1, \dots, N-1, \\ \alpha\beta^{-1} = \omega^{2N(2j+\frac{1-\lambda}{2})} & \text{for some } j = 0, 1, \dots, n-1. \end{cases}$$

Similarly, we see that the set $J = \{ (\gamma, \xi) \in \mathbf{k} \times \mathbf{k} \mid \gamma^2 = \xi^2, \gamma^{2N} = 1 \}$ can be expressed as

$$J = \{ (\omega^{4i}, \omega^{4i}) \mid i = 0, 1, \dots, 2N-1 \} \cup \{ (\omega^{4i}, -\omega^{4i}) \mid i = 0, 1, \dots, 2N-1 \}.$$

We put $A = A_{Nn}^{\nu\lambda}$.

(1) We consider the case of $g = x_{11}^{2s} \pm x_{12}^{2s}$. If $n \geq 3$, then by Lemma 5.10(1)(i)

$$\begin{aligned}
P_{A^*, kg}(x) &= \prod_{(\alpha, \beta) \in I_{\nu\lambda}} (x - (\alpha\beta)^{-2s^2}) \\
&= \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - \omega^{-4n(2i + \frac{1-\nu}{2})s^2}) \cdot \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - \omega^{-4n(2i + \frac{1-\nu}{2})s^2}) \\
&= \prod_{i=0}^{N-1} (x - \omega^{-4n(2i + \frac{1-\nu}{2})s^2})^{2n},
\end{aligned}$$

and if $n = 2$, then by Lemma 5.10(2)(i)

$$\begin{aligned}
P_{A^*, kg}(x) &= \prod_{(\alpha, \beta) \in I_{\nu\lambda}} (x - (\alpha\beta)^{-2s^2}) \cdot \prod_{(\gamma, \xi) \in J} (x - \gamma^{-4s^2}) \\
&= \prod_{i=0}^{N-1} (x - \omega^{-8(2i + \frac{1-\nu}{2})s^2})^4 \cdot \prod_{i=0}^{2N-1} (x - \omega^{-16is^2})^2 \\
&= \prod_{i=0}^{N-1} (x - \omega^{-8(2i + \frac{1-\nu}{2})s^2})^4 \cdot \prod_{i=0}^{N-1} (x - \omega^{-16is^2})^4.
\end{aligned}$$

Next we consider the case of $g = x_{11}^{2s+1} \chi_{22}^{n-1} \pm \sqrt{\lambda} x_{12}^{2s+1} \chi_{21}^{n-1}$. If $n \geq 3$, then by Lemma 5.10(1)(i)

$$\begin{aligned}
P_{A^*, kg}(x) &= \prod_{(\alpha, \beta) \in I_{\nu\lambda}} (x - \nu^n (\alpha\beta)^{-2s^2 - 2sn - n^2} \alpha^{n^2}) \\
&= \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - (-1)^{nj} \nu^n \omega^{-n(2i + \frac{1-\nu}{2})(2s+n)^2 + n^2 N \frac{1-\lambda}{2}}) \\
&\quad \times \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - (-1)^n (-1)^{nj} \nu^n \omega^{-n(2i + \frac{1-\nu}{2})(2s+n)^2 + n^2 N \frac{1-\lambda}{2}}) \\
&= \begin{cases} \prod_{i=0}^{N-1} (x^2 - \omega^{-2n(2s+n)^2(2i + \frac{1-\nu}{2})} (-1)^{\frac{1-\lambda}{2}n})^n & (n \text{ is odd}), \\ \prod_{i=0}^{N-1} (x - \omega^{-n(2s+n)^2(2i + \frac{1-\nu}{2})} (-1)^{\frac{n}{2} \frac{1-\lambda}{2}})^{2n} & (n \text{ is even}), \end{cases}
\end{aligned}$$

and if $n = 2$, then by Lemma 5.10(2)(i)

$$\begin{aligned}
P_{A^*, kg}(x) &= \prod_{(\alpha, \beta) \in I_{\nu\lambda}} (x - (\alpha\beta)^{-2s^2 - 4s - 4} \alpha^4) \cdot \prod_{(\gamma, \xi) \in J} (x - \gamma^{-4(s+1)^2} \lambda) \\
&= \prod_{i=0}^{N-1} (x - \omega^{-4(s+1)^2(2i + \frac{1-\nu}{2})} (-1)^{\frac{1-\lambda}{2}4})^4 \cdot \prod_{i=0}^{2N-1} (x - \omega^{-16i(s+1)^2} \lambda)^2 \\
&= \prod_{i=0}^{N-1} (x - \omega^{-4(s+1)^2(2i + \frac{1-\nu}{2})} (-1)^{\frac{1-\lambda}{2}4})^4 \cdot \prod_{i=0}^{N-1} (x - \omega^{-16i(s+1)^2} \lambda)^4.
\end{aligned}$$

(2) If $n \geq 3$, then by Lemma 5.10(1)(ii),

$$\begin{aligned}
P_{A^*, V_{st}}(x) &= \prod_{(\alpha, \beta) \in I_{\nu\lambda}} (x - \nu^t \alpha^{t^2} (\alpha\beta)^{-2s^2 - 2st - t^2}) \\
&= \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - \nu^t \omega^{n(2i + \frac{1-\nu}{2})(-4s^2 - 4st - t^2) + N(2j + \frac{1-\lambda}{2})t^2}) \\
&\quad \times \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - (-1)^t \nu^t \omega^{n(2i + \frac{1-\nu}{2})(-4s^2 - 4st - t^2) + N(2j + \frac{1-\lambda}{2})t^2}) \\
&= \begin{cases} \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x^2 - \omega^{-2n(2s+t)^2(2i + \frac{1-\nu}{2}) + 2Nt^2(2j + \frac{1-\lambda}{2})}) & (t \text{ is odd}) \\ \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - \omega^{-n(2s+t)^2(2i + \frac{1-\nu}{2}) + Nt^2(2j + \frac{1-\lambda}{2})})^2 & (t \text{ is even}) \end{cases} \\
&= \begin{cases} \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x^2 - \omega^{-2n(2s+t)^2(2i + \frac{1-\nu}{2}) + 2Nt^2(2(n-j) + \frac{1-\lambda}{2})}) & (t \text{ is odd}) \\ \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - \omega^{-n(2s+t)^2(2i + \frac{1-\nu}{2}) + Nt^2(2(n-j) + \frac{1-\lambda}{2})})^2 & (t \text{ is even}) \end{cases} \\
&= \begin{cases} \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x^2 - \omega^{-2n(2s+t)^2(2i + \frac{1-\nu}{2}) - 2Nt^2(2j + \frac{\lambda-1}{2})}) & (t \text{ is odd}) \\ \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - \omega^{-n(2s+t)^2(2i + \frac{1-\nu}{2}) - Nt^2(2j + \frac{\lambda-1}{2})})^2 & (t \text{ is even}), \end{cases}
\end{aligned}$$

and if $n = 2$, then by Lemma 5.10(2)(ii),

$$\begin{aligned}
P_{A^*, V_{s1}}(x) &= \prod_{(\alpha, \beta) \in I_{\nu\lambda}} (x - \nu \alpha (\alpha\beta)^{-2s^2 - 2s - 1}) \cdot \prod_{(\gamma, \xi) \in J} (x - \gamma^{-(2s+1)^2}) \\
&= \prod_{i=0}^{N-1} \prod_{j=0}^1 (x^2 - \omega^{-4(2i + \frac{1-\nu}{2})(2s+1)^2 + 2N(2j + \frac{1-\lambda}{2})}) \cdot \prod_{i=0}^{2N-1} (x - \omega^{-4i(2s+1)^2})^2 \\
&= \prod_{i=0}^{N-1} (x^4 - \omega^{-8(2i + \frac{1-\nu}{2})(2s+1)^2 + 2N(1-\lambda)}) \cdot \prod_{i=0}^{N-1} (x^2 - \omega^{-8i(2s+1)^2})^2.
\end{aligned}$$

□

In the case where N is odd and $\nu = +$, if λ and n satisfy the condition

(A) $\lambda = -1$, or

(B) $\lambda = 1$, and n is odd,

then the Hopf algebra $A_{Nn}^{+\lambda}$ is self-dual (see Corollary 6.9 in the next section). Therefore, by using Proposition 4.5 we have:

Corollary 5.12. *Let $N \geq 1$ be an odd integer and $\omega \in \mathbf{k}$ a primitive $4nN$ -th root of unity. Suppose that λ and n satisfy the above condition (A) or (B). Then*

$$P_{A_{Nn}^{+\lambda}}^{(1)}(x) = \begin{cases} \prod_{s=0}^{N-1} \prod_{i=0}^{N-1} (x - \omega^{-8nis^2})^{4n} (x^2 - \omega^{-4in(2s+1)^2} (-1)^{\frac{1-\lambda}{2}})^{2n} & (n \text{ is odd}), \\ \prod_{s=0}^{N-1} \prod_{i=0}^{N-1} (x - \omega^{-8nis^2})^{4n} (x - \omega^{-8ins^2} (-1)^{\frac{n}{2}})^{4n} & (n \geq 4 \text{ is even}), \\ \prod_{s=0}^{N-1} \prod_{i=0}^{N-1} (x - \omega^{-16is^2})^{16} (x + \omega^{-8is^2})^8 (x + \omega^{-16is^2})^8 & (n = 2), \end{cases}$$

$$P_{A_{Nn}^{+\lambda}}^{(2)}(x) = \begin{cases} \prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n-\epsilon(n)}{2}} \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x^2 - \omega^{-4in(2s+1)^2 - 2N(2t-1)^2(2j+\frac{\lambda-1}{2})}) \\ \times \prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n-2+\epsilon(n)}{2}} \prod_{i=0}^{N-1} \prod_{j=0}^{n-1} (x - \omega^{-8ins^2 - 4Nt^2(2j+\frac{\lambda-1}{2})})^2 & (n \geq 3), \\ \prod_{s=0}^{N-1} \prod_{i=0}^{N-1} (x^4 + \omega^{-16i(2s+1)^2}) (x^2 - \omega^{-8i(2s+1)^2})^2 & (n = 2), \end{cases}$$

where

$$\epsilon(n) = \begin{cases} 0 & (n \text{ is even}), \\ 1 & (n \text{ is odd}). \end{cases}$$

From the above corollary the polynomial invariants of the Kac-Paljutkin algebra $K_8 \cong A_{12}^{+-}$ are computed, again.

5.3 The group Hopf algebra $\mathbf{k}[G_{Nn}]$

If N is odd, $n \geq 2$, and $\lambda = \pm 1$, then $A_{Nn}^{+\lambda}$ is isomorphic to the group algebra of the finite group

$$G = \langle h, t, w \mid t^2 = h^{2N} = 1, w^n = h^{(n+\frac{\lambda-1}{2})N}, tw = w^{-1}t, ht = th, hw = wh \rangle$$

as an algebra (for the proof see Proposition 6.1 in the next section). The order of G is $4nN$. If $(n, \lambda) = (\text{even}, 1)$ or $(n, \lambda) = (\text{odd}, -1)$, then the group G is isomorphic to the direct product $D_{2n} \times C_{2N}$. If $(n, \lambda) = (\text{even}, -1)$ or $(n, \lambda) = (\text{odd}, 1)$, then G is isomorphic to the semidirect product of

$$H := \langle w, h \mid h^{2N} = 1, w^n = h^N, wh = hw \rangle$$

and C_2 , where the action of $C_2 = \langle t \rangle$ on H is given by $t \cdot w := w^{-1}$ and $t \cdot h := h$. In particular, when $N = 1$, the group G is the dihedral group of order $4n$.

We shall determine the universal R -matrices of the group Hopf algebra $\mathbf{k}[G]$, and calculate the polynomial invariants of it in the case where $(n, \lambda) = (\text{even}, -1)$ or $(n, \lambda) = (\text{odd}, 1)$. In this case, G coincides with the group

$$G_{Nn} = \langle h, t, w \mid t^2 = h^{2N} = 1, w^n = h^N, tw = w^{-1}t, ht = th, hw = wh \rangle.$$

Lemma 5.13. *Let N be an odd integer, and $n \geq 2$ an integer.*

(1) *If $n \geq 3$, then the finite group G_{Nn} has a unique maximal commutative normal subgroup, which is given by $H = \langle h, w \rangle$.*

(2) *If $n = 2$, then the finite group G_{Nn} has exactly three maximal commutative normal subgroups, which are given by $H_1 = \langle h, w \rangle$, $H_2 = \langle h, t \rangle$ and $H_3 = \langle h, tw \rangle$.*

Proof. We set $G = G_{Nn}$. It is clear that $H (= H_1)$ is a commutative and normal subgroup of G , and it is not hard to show that H is maximal between commutative subgroups. Hence H is a maximal commutative normal subgroup of G . In the case of $n = 2$ we see that H_2 and H_3 are also commutative and normal subgroups of G , and maximal between commutative subgroups.

We show that the converse is true.

(1) Let K be a maximal commutative normal subgroup K of $G = G_{Nn}$. Suppose that $K \not\subset H$. Then $K \cap (G - H) \neq \emptyset$. So, if we take an element $tw^i h^j \in K \cap (G - H)$ ($0 \leq i < n$, $0 \leq j < N$), then $w(tw^i h^j)w^{-1} = tw^{i-2} h^j \in K$, that is, $tw^i h^j \in K$ implies $h^{-j} w^{-i+2} t = (tw^{i-2} h^j)^{-1} \in K$. Since K is commutative, we have the equation

$$w^2 = h^{-j} w^{-i+2} t \cdot tw^i h^j = tw^i h^j \cdot h^{-j} w^{-i+2} t = w^{-2} = w^{2n-2} = w^{(n-2)+n} = w^{n-2} h^N.$$

This is a contradiction since $n \geq 3$. Thus $K \subset H$. This implies that $K = H$ from maximality of K .

(2) Let K be a maximal commutative normal subgroup K of $G = G_{Nn}$. Then $\langle h \rangle \subset K$ holds from maximality of K since $K\langle h \rangle$ is a commutative and normal subgroup of G . If $K \subset H_1$, then $K = H_1$ since H_1 is a maximal commutative normal subgroup of G . So, we suppose that $K \not\subset H_1$. Then $tw^i h^j \in K$ for some i, j ($i = 0, 1$, $j = 0, 1, \dots, N-1$). Since $\langle h \rangle \subset K$, we have $tw^i \in K$.

If $i = 0$, then $t \in K$, and hence $H_2 \subset K$. By maximality of H_2 , we see that $K = H_2$. By the same argument, we see that if $i = 1$, then $K = H_3$. Thus there is no maximal commutative normal subgroup of G except for H_1, H_2, H_3 . \square

In what follows, we assume that the characteristic $\text{ch}(\mathbf{k})$ does not divide $2nN$. To determine the universal R -matrices of $\mathbf{k}[H]$, we use the basis consisting of the primitive idempotents of $\mathbf{k}[H]$.

Lemma 5.14. *Let $N \geq 1$ be an odd integer, and $n \geq 2$ an integer. Let H be the commutative group of order $2nN$ defined by $H = \langle h, w \mid h^{2N} = 1, w^n = h^N, hw = wh \rangle$, and ω a primitive $4nN$ -th root of unity in \mathbf{k} . For $i, k \in \mathbb{Z}$, we set*

$$E_{ik} = \frac{1}{2nN} \sum_{j=0}^{n-1} \sum_{l=0}^{2N-1} \omega^{-2Nj(k+2i)-2nkl} w^j h^l \in \mathbf{k}[H].$$

Then $\{ E_{ik} \mid i = 0, 1, \dots, n-1, k = 0, 1, \dots, 2N-1 \}$ is the set of primitive idempotents of

$\mathbf{k}[H]$, and the following equations hold: for all $i, j, k, l \in \mathbb{Z}$

$$E_{i+n,k} = E_{ik}, \quad E_{i-N,k+2N} = E_{ik}, \quad (5.4)$$

$$E_{ik}E_{jl} = \delta_{kl}^{(2N)} \delta_{k+2i,l+2j}^{(2n)} E_{jl} = \delta_{kl}^{(2N)} \delta_{k+2i,l+2j}^{(2n)} E_{ik}, \quad (5.5)$$

where

$$\delta_{kl}^{(m)} = \begin{cases} 1 & (k \equiv l \pmod{m}) \\ 0 & (k \not\equiv l \pmod{m}) \end{cases}$$

for $m = 2N$ or $m = 2n$. Furthermore, the coproduct Δ , the counit ε , and the antipode S of the group Hopf algebra $\mathbf{k}[H]$ are given as follows:

$$\Delta(E_{ik}) = \sum_{\substack{0 \leq p, q \leq 2N-1 \\ p+q \equiv k \pmod{2N}}} \sum_{\substack{0 \leq a, b \leq n-1 \\ a+b + \frac{-k+p+q}{2} \equiv i \pmod{n}}} E_{ap} \otimes E_{bq}, \quad (5.6)$$

$$\varepsilon(E_{ik}) = \delta_{i,0} \delta_{k,0}, \quad (5.7)$$

$$S(E_{ik}) = E_{-i,-k}. \quad (5.8)$$

Proof. For integers i and k , let χ_{jk} be the group homomorphism from H to \mathbf{k} defined by $\chi_{ik}(w) = \omega^{2N(k+2i)}$, $\chi_{ik}(h) = \omega^{2nk}$. Then the set $\{\chi_{ik} \mid i = 0, 1, \dots, n-1, k = 0, 1, \dots, 2N-1\}$ consists of all irreducible characters of H . So,

$$\frac{1}{2nN} \sum_{j=0}^{n-1} \sum_{l=0}^{2N-1} \chi_{ik}(w^{-j}h^{-l}) w^j h^l = \frac{1}{2nN} \sum_{j=0}^{n-1} \sum_{l=0}^{2N-1} \omega^{-2Nj(k+2i)-2nkl} w^j h^l = E_{jk}$$

is a primitive idempotent of $\mathbf{k}[H]$, and the set $\{E_{ik}\}$ consists of all primitive idempotents of $\mathbf{k}[H]$. By definition the equations (5.4) and (5.7) are obtained immediately, and the equations (5.5), (5.6) and (5.8) follow from that $w^j h^l$ is written as

$$w^j h^l = \sum_{i=0}^{n-1} \sum_{k=0}^{2N-1} \omega^{2Nj(2i+k)+2nkl} E_{ik}, \quad (5.9)$$

which comes from orthogonality of characters. \square

Lemma 5.15. Let $N \geq 1$ be an odd integer, and $n \geq 2$ an integer. Let H be the commutative group of order $2nN$ defined in Lemma 5.14, and $\omega \in \mathbf{k}$ a primitive $4nN$ -th root of unity. Then any universal R -matrix R of $\mathbf{k}[H]$ is given by

$$R = \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{2N-1} \nu^{kl} \omega^{2aN(2i+k)(2j+l)+2n(qkl+2pjk+2rij)} E_{ik} \otimes E_{jl} \quad (5.10)$$

for some $\nu \in \{\pm 1\}$, $a \in \{0, 1, \dots, n-1\}$ and $p, q, r \in \{0, 1, \dots, N-1\}$ such that pn, rn are multiples of N , where $\{E_{ik}\}$ is the set of primitive idempotents of $\mathbf{k}[H]$ defined in Lemma 5.14. Conversely, the above R given by (5.10) is a universal R -matrix of $\mathbf{k}[H]$.

Proof. Let R be an element of $\mathbf{k}[H] \otimes \mathbf{k}[H]$, and write R in the form

$$R = \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{2N-1} R_{jl}^{ik} E_{ik} \otimes E_{jl} \quad (R_{jl}^{ik} \in \mathbf{k}).$$

We treat the indices i and j of R_{jl}^{ik} as modulo n , therefore R_{jl}^{ik} has a meaning for all integers i and j . For $0 \leq m \leq 4N - 1$, we define $\delta(m)$ by

$$\delta(m) = \begin{cases} 0 & (0 \leq m \leq 2N - 1), \\ 1 & (2N \leq m \leq 4N - 1). \end{cases}$$

Then we have

$$\begin{aligned} (\Delta \otimes \text{id})(R) &= \sum_{j,a,b=0}^{n-1} \sum_{l,p,q=0}^{2N-1} R_{jl}^{a+b+N\delta(p+q), p+q-2N\delta(p+q)} E_{ap} \otimes E_{bq} \otimes E_{jl}, \\ R_{13}R_{23} &= \sum_{j,a,b=0}^{n-1} \sum_{l,p,q=0}^{2N-1} R_{jl}^{ap} R_{jl}^{bq} E_{ap} \otimes E_{bq} \otimes E_{jl}. \end{aligned}$$

Hence $(\Delta \otimes \text{id})(R) = R_{13}R_{23}$ if and only if

$$R_{jl}^{a+b+N\delta(p+q), p+q-2N\delta(p+q)} = R_{jl}^{ap} R_{jl}^{bq} \quad (5.11)$$

for all $j, a, b = 0, 1, \dots, n - 1$ and $l, p, q = 0, 1, \dots, 2N - 1$. Similarly, $(\text{id} \otimes \Delta)(R) = R_{13}R_{12}$ if and only if

$$R_{jl}^{ik} R_{jl}^{a+b+N\delta(p+q), p+q-2N\delta(p+q)} = R_{jl}^{ik} R_{jl}^{ap} \quad (5.12)$$

for $i, a, b = 0, 1, \dots, n - 1$ and $k, p, q = 0, 1, \dots, 2N - 1$, and also we have $(\varepsilon \otimes \text{id})(R) = (\text{id} \otimes \varepsilon)(R) = 1$ if and only if

$$R_{jl}^{00} = R_{00}^{jl} = 1 \quad (5.13)$$

for $j = 0, 1, \dots, n - 1$ and $l = 0, 1, \dots, 2N - 1$. Thus R is a universal R -matrix of $\mathbf{k}[H]$ if and only if the equations (5.11), (5.12), (5.13) hold. From the equations (5.11) and (5.12), R_{jl}^{ik} can be expressed as the form

$$R_{jl}^{ik} = (R_{01}^{01})^{kl} (R_{10}^{01})^{jk} (R_{01}^{10})^{il} (R_{10}^{10})^{ij}.$$

Since $(R_{01}^{10})^n = R_{01}^{n0} = R_{00}^{00} = 1$ and $(R_{10}^{01})^n = R_{n0}^{01} = R_{00}^{01} = 1$ by (5.11), we see that R_{01}^{10} and R_{10}^{01} are can be written as

$$R_{01}^{10} = \omega^{4aN}, \quad R_{10}^{01} = \omega^{4bN} \quad (0 \leq a, b \leq n - 1). \quad (5.14)$$

By using the equations (5.11) and (5.12), repeatedly, we have

$$\begin{cases} (R_{01}^{01})^{2N} = (R_{01}^{01})^{2N-2} R_{01}^{02} = \dots = R_{01}^{01} R_{01}^{0,2N-1} = R_{01}^{N0} = (R_{01}^{10})^N = \omega^{4aN^2}, \\ (R_{01}^{01})^{2N} = (R_{01}^{01})^{2N-2} R_{02}^{01} = \dots = R_{01}^{01} R_{0,2N-1}^{01} = R_{N0}^{01} = (R_{10}^{01})^N = \omega^{4bN^2}. \end{cases}$$

Therefore $\omega^{4bN} = \omega^{4aN+4pn}$ must be required for some $0 \leq p \leq N-1$ such that pn is a multiple of N . From the equation $(R_{01}^{01})^{2N} = \omega^{4aN^2}$, we may set $(R_{01}^{01})^2 = \omega^{4aN+4qn}$ ($0 \leq q \leq N-1$), and hence

$$R_{01}^{01} = \pm \omega^{2aN+2qn}. \quad (5.15)$$

By using the equation (5.11), repeatedly, we have $(R_{10}^{10})^N = R_{N0}^{10} = (R_{01}^{10})^{2N} = \omega^{8aN^2}$. So, R_{10}^{10} can be expressed as

$$R_{10}^{10} = \omega^{8aN+4rn} \quad (5.16)$$

for some $0 \leq r \leq N-1$ such that rn is a multiple of N . From (5.14), (5.15) and (5.16) we see that a universal R -matrix R of $\mathbf{k}[H]$ is written in the form

$$R = \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{2N-1} R_{jl}^{ik} E_{ik} \otimes E_{jl}, \quad R_{jl}^{ik} = \nu^{kl} \omega^{2aN(2i+k)(2j+l)+2n(qkl+2pjk+2rij)}$$

for some $\nu \in \{\pm 1\}$, $a \in \{0, 1, \dots, n-1\}$ and $p, q, r \in \{0, 1, \dots, N-1\}$ that pn, rn are multiples of N .

Conversely, it is not hard to check that $R \in \mathbf{k}[H] \otimes \mathbf{k}[H]$ which is given by the form above is a universal R -matrix of $\mathbf{k}[H]$. \square

By use of Lemma 5.1 and Lemma 5.15 one can determine the universal R -matrices of $\mathbf{k}[G_{Nn}]$.

Proposition 5.16. *Let $N \geq 1$ be an odd integer, and $n \geq 2$ an integer. Let ω be a primitive $4nN$ -th root of unity in \mathbf{k} , and $\{E_{ik}\}$ be the set of primitive idempotent of $\mathbf{k}[H]$ defined in Lemma 5.14. Then for any $\nu \in \{\pm 1\}$, $a \in \{0, 1, \dots, n-1\}$, $q \in \{0, 1, \dots, N-1\}$,*

$$R_{aq\nu} := \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{2N-1} \nu^{kl} \omega^{2aN(2i+k)(2j+l)+2qkln} E_{ik} \otimes E_{jl} \quad (5.17)$$

is a universal R -matrix of the group Hopf algebra $\mathbf{k}[G_{Nn}]$. Furthermore,

- $R_{aq\nu}$ is a universal R -matrix of the group Hopf algebra $\mathbf{k}[\langle h \rangle]$ if and only if $a = 0$, and
- if $n \geq 3$, then any universal R -matrix is given by the above form, therefore, the number of the universal R -matrices of $\mathbf{k}[G_{Nn}]$ is $2nN$.

Proof. Let R be a universal R -matrix of $\mathbf{k}[H]$, where H is the subgroup of G_{Nn} defined in Lemma 5.15, and write it in the form

$$R = \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{2N-1} R_{jl}^{ik} E_{ik} \otimes E_{jl}.$$

By using $E_{ik}t = tE_{-i-k,k}$ we have

$$\begin{aligned} \Delta^{\text{cop}}(t) \cdot R &= \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{2N-1} R_{jl}^{ik} tE_{ik} \otimes tE_{jl}, \\ R \cdot \Delta(t) &= \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{2N-1} R_{-j-l,l}^{-i-k,k} tE_{ik} \otimes tE_{jl}. \end{aligned}$$

Hence R is a universal R -matrix of $\mathbf{k}[G_{Nn}]$ if and only if $R_{-j-l,l}^{-i-k,k} = R_{jl}^{ik}$ for all i, j, k, l . Since R is a universal R -matrix of $\mathbf{k}[H]$, R_{jl}^{ik} is written in the form

$$R_{jl}^{ik} = \nu^{kl} \omega^{2aN(2i+k)(2j+l)+2n(qkl+2pjk+2rij)}$$

for some $a \in \{0, 1, \dots, n-1\}$ and $p, q, r \in \{0, 1, \dots, N-1\}$. Therefore, we have

$$R_{-j-l,l}^{-i-k,k} = R_{jl}^{ik} \iff \omega^{2n(-2p(2j+l)k+2r(kj+il+kl))} = 1.$$

Considering the equations in R.H.S. for $(i, j, k, l) = (1, 0, 0, 1)$ and $(i, j, k, l) = (0, 0, 1, 1)$, we see that R is a universal R -matrix of $\mathbf{k}[G_{Nn}]$ if and only if $\omega^{4pn} = \omega^{4rn} = 1$. This condition is equivalent to that the both p and r are multiples of N . It follows from $0 \leq p, r \leq N-1$ that $p = r = 0$. \square

Proposition 5.17. *Let $N \geq 1$ be an odd integer, and let ω be a primitive $8N$ -th root of unity in a field \mathbf{k} whose characteristic does not divide $2N$. Then the number of universal R -matrices of the group Hopf algebra $\mathbf{k}[G_{N2}]$ is $8N$, and they are given by the list below.*

- universal R -matrices of $\mathbf{k}[\langle h \rangle]$:

$$R_d = \sum_{k,l=0}^{2N-1} \omega^{4dkl} E_k \otimes E_l \quad (d = 0, 1, \dots, 2N-1),$$

where $E_k = \frac{1}{2N} \sum_{l=0}^{2N-1} \omega^{-4kl} h^l$.

- universal R -matrices of $\mathbf{k}[H_1]$, where $H_1 = \langle h, w \rangle$:

$$R_{1q\nu} = \sum_{i,j=0,1} \sum_{k,l=0}^{2N-1} \nu^{kl} \omega^{2N(2i+k)(2j+l)+4qkl} E_{ik} \otimes E_{jl} \quad (q = 0, 1, \dots, N-1, \nu = \pm 1),$$

where $E_{ik} = \frac{1}{4N} \sum_{j=0,1} \sum_{l=0}^{2N-1} (-1)^{ij} \omega^{-2Njk-4kl} w^j h^l$.

- universal R -matrices of $\mathbf{k}[H_2]$, where $H_2 = \langle h, t \rangle$:

$$R_d^{(1)} := R_{0N1d}^{\mathbf{k}[H_2]} = \sum_{i,j=0,1} \sum_{k,l=0}^{2N-1} (-1)^{jk+il} \omega^{4dkl} E_{ik} \otimes E_{jl} \quad (d = 0, 1, \dots, 2N-1), \quad (5.18)$$

where $E_{ik} = \frac{1}{4N} \sum_{j=0,1} \sum_{l=0}^{2N-1} (-1)^{ij} \omega^{-4kl} t^j h^l$.

- universal R -matrices of $\mathbf{k}[H_3]$, where $H_3 = \langle h, tw \rangle$:

$$R_d^{(2)} := R_{0N1d}^{\mathbf{k}[H_3]} = \sum_{i,j=0,1} \sum_{k,l=0}^{2N-1} (-1)^{jk+il} \omega^{4dkl} E_{ik} \otimes E_{jl} \quad (d = 0, 1, \dots, 2N-1), \quad (5.19)$$

where $E_{ik} = \frac{1}{4N} \sum_{j=0,1} \sum_{l=0}^{2N-1} (-1)^{ij} \omega^{-4kl} (tw)^j h^l$.

Proof. By Proposition 5.16 it is sufficient to determine the universal R -matrices of $\mathbf{k}[G_{N2}]$ which come from that of $\mathbf{k}[H_2]$ or $\mathbf{k}[H_3]$. By Lemma 5.2 it follows from $H_i \cong C_2 \times C_{2N}$ for $i = 2, 3$ that a universal R -matrix of $\mathbf{k}[H_i]$ is given by

$$R_{pqrs}^{\mathbf{k}[H_i]} = \sum_{i,j=0}^{m-1} \sum_{k,l=0}^{n-1} (-1)^{(pi+rk)j} \omega^{2(sk+qil)} E_{ik} \otimes E_{jl},$$

where $p, r \in \{0, 1\}$, $q \in \{0, N\}$, $s \in \{0, 1, \dots, 2N-1\}$.

Let us consider the case of $i = 2$ and $R = R_{pqrs}^{\mathbf{k}[H_2]}$. We set $R_{jl}^{ik} = (-1)^{j(pi+rk)} \omega^{2l(sk+qi)}$. Then by using $E_{ik}w = wE_{i+k,k}$, we have

$$\begin{aligned} \Delta^{\text{cop}}(w) \cdot R &= R \cdot \Delta(w) \iff R_{j-l,l}^{i-k,k} = R_{jl}^{ik} \text{ for all } i, j, k, l \\ &\iff (-1)^{-(j-l)pk-l(pi+rk)} \omega^{-2lqk} = 1 \text{ for all } i, j, k, l \\ &\iff (p, q, r) = (0, 0, 0) \text{ or } (p, q, r) = (0, N, 1). \end{aligned}$$

Thus $R_{pqrs}^{\mathbf{k}[H_2]}$ is a universal R -matrix of $\mathbf{k}[G_{N2}]$ if and only if $(p, q, r) = (0, 0, 0)$ or $(p, q, r) = (0, N, 1)$. It is easy proved that $R_{000s}^{\mathbf{k}[H_2]}$ is a universal R -matrix of $\mathbf{k}[\langle h \rangle]$, and $R_{0N1s}^{\mathbf{k}[H_2]}$ is not. By a similar manner, it is shown that a universal R -matrix $R_{pqrs}^{\mathbf{k}[H_3]}$ of $\mathbf{k}[H_3]$ is a universal R -matrix of $\mathbf{k}[G]$ if and only if $(p, q, r) = (0, 0, 0), (0, N, 1)$, and $R_{pqrs}^{\mathbf{k}[H_3]}$ is that of $\mathbf{k}[\langle h \rangle]$ if and only if $(p, q, r) = (0, 0, 0)$. \square

Lemma 5.18. *Let $N \geq 1$ be an odd integer, and $n \geq 2$ an integer.*

(1) *The Drinfel'd element $u_{aq\nu}$ associated to $R_{aq\nu}$ in Proposition 5.16 is given by*

$$u_{aq\nu} = \sum_{i=0}^{n-1} \sum_{k=0}^{2N-1} \nu^k \omega^{-2aN(2i+k)^2-2nqk^2} E_{ik},$$

where $\{E_{ik}\}$ be the set of primitive idempotents of $\mathbf{k}[H]$ defined in Lemma 5.14.

(2) *In the case of $n = 2$, for each $i = 1, 2$ the Drinfel'd element $u_d^{(i)}$ associated to $R_d^{(i)}$ given by (5.18) and (5.19) is given by*

$$u_d^{(i)} = \sum_{k=0}^{2N-1} \omega^{-4dk^2} E_k,$$

where $E_k = \frac{1}{2N} \sum_{l=0}^{2N-1} \omega^{-4kl} h^l$.

Proof. (1) By definition,

$$u_{aq\nu} = \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{2N-1} \nu^{kl} \omega^{2aN(2i+k)(2j+l)+2qkln} \delta_{k,-l}^{(2N)} \delta_{2i+k,-2j-l}^{(2n)} E_{ik}.$$

For a fixed integer $k \in \{0, 1, \dots, 2N-1\}$ there is a unique integer $l \in \{0, 1, \dots, 2N-1\}$ satisfying $-l \equiv k \pmod{2N}$, and that is given by

$$l = \begin{cases} 2N - k & (k = 1, \dots, 2N-1), \\ 0 & (k = 0), \end{cases}$$

and under this condition, for a fixed integer $i \in \{0, 1, \dots, n-1\}$ there is a unique integer $j \in \{0, 1, \dots, n-1\}$ satisfying $-2j - l \equiv 2i + k \pmod{2n}$, and that is given by

$$j \equiv \begin{cases} -N - i & (k = 1, \dots, 2N-1), \\ -i & (k = 0) \end{cases} \pmod{n}.$$

Thus we have

$$\begin{aligned} u_{aq\nu} &= \sum_{i=0}^{n-1} \sum_{k=1}^{2N-1} \nu^k \omega^{-2aN(2i+k)^2 - 2qk^2n} E_{ik} + \sum_{i=0}^{n-1} \omega^{-8ai^2N} E_{i0} \\ &= \sum_{i=0}^{n-1} \sum_{k=0}^{2N-1} \nu^k \omega^{-2aN(2i+k)^2 - 2qk^2n} E_{ik}. \end{aligned}$$

(2) By definition,

$$u_d^{(1)} = \sum_{i,j=0,1} \sum_{k,l=0}^{2N-1} (-1)^{jk+il} \omega^{4dkl} S(E_{jl}) E_{ik} = \sum_{i=0,1} \sum_{k=0}^{2N-1} \omega^{-4dk^2} E_{ik} = \sum_{k=0}^{2N-1} \omega^{-4dk^2} E_k.$$

By a similar computation, we have the formula for $u_d^{(2)}$. \square

Let $\omega \in \mathbf{k}$ be a primitive $4nN$ -th root of unity. Then a full set of non-isomorphic simple left $\mathbf{k}[G_{Nn}]$ -modules is given by

$$\begin{aligned} &\{ V_{ijk} \mid i, j = 0, 1, \ k = 0, 2, \dots, 2N-2 \} \\ &\cup \{ V_{jk} \mid k = 0, 1, \dots, 2N-1, \ j = 1, 2, \dots, n-1, \ j \equiv k \pmod{2} \}, \end{aligned}$$

where the action χ_{ijk} of $\mathbf{k}[G_{Nn}]$ on $V_{ijk} = \mathbf{k}$ is given by

$$\chi_{ijk}(t) = (-1)^i, \ \chi_{ijk}(w) = (-1)^j, \ \chi_{ijk}(h) = \begin{cases} \omega^{2kn} & (n \text{ is even}), \\ \omega^{2(j+k)n} & (n \text{ is odd}), \end{cases} \quad (5.20)$$

and the left action ρ_{jk} of $\mathbf{k}[G_{Nn}]$ on $V_{jk} = \mathbf{k} \oplus \mathbf{k}$ is given by

$$\rho_{jk}(t) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \rho_{jk}(w) = \begin{pmatrix} \omega^{2jN} & 0 \\ 0 & \omega^{-2jN} \end{pmatrix}, \ \rho_{jk}(h) = \begin{pmatrix} \omega^{2kn} & 0 \\ 0 & \omega^{2kn} \end{pmatrix}. \quad (5.21)$$

Lemma 5.19. *For each universal R -matrix R of $\mathbf{k}[G_{Nn}]$, the R -dimensions of the simple left $\mathbf{k}[G_{Nn}]$ -modules V_{ijk} and V_{jk} are given as follows.*

(1) For $n \geq 2$,

$$\underline{\dim}_{R_{aq\nu}} V_{ijk} = \begin{cases} \omega^{-2nqk^2} & (n \text{ is even}), \\ \nu^j (-1)^{aj} \omega^{-2nq(j+k)^2} & (n \text{ is odd}), \end{cases} \quad (5.22)$$

$$\underline{\dim}_{R_{aq\nu}} V_{jk} = 2\nu^k \omega^{-2nqk^2 - 2Naj^2}. \quad (5.23)$$

(2) For $n = 2$,

$$\begin{aligned} \underline{\dim}_{R_d^{(1)}} V_{ijk} &= \underline{\dim}_{R_d^{(2)}} V_{ijk} = \omega^{-4dk^2}, \\ \underline{\dim}_{R_d^{(1)}} V_{1k} &= \underline{\dim}_{R_d^{(2)}} V_{1k} = 2\omega^{-4dk^2}. \end{aligned}$$

Proof. (1) Let n be an even integer. Since

$$\begin{aligned}\chi_{ijk}(E_{ml}) &= \frac{1}{2nN} \sum_{b=0}^{n-1} \sum_{p=0}^{2N-1} \omega^{-2bN(l+2m)-2lpn} (-1)^{jb} (\omega)^{2kpn} \\ &= \delta_{k,l} \frac{1}{n} \sum_{b=0}^{n-1} \omega^{4bN(\frac{nj-k}{2}-m)} \\ &= \delta_{k,l} \delta_{\frac{nj-k}{2}, m}^{(n)},\end{aligned}$$

we have

$$\chi_{ijk}(u_{aq\nu}) = \sum_{m=0}^{n-1} \nu^k \omega^{-2aN(2m+k)^2-2qk^2n} \delta_{\frac{nj-k}{2}, m}^{(n)} = \sum_{m=0}^{n-1} \omega^{-2aN(2m+k)^2-2qk^2n} \delta_{\frac{nj-k}{2}, m}^{(n)}.$$

Since there is a unique integer in $\{0, 1, \dots, n-1\}$ which is equal to $\frac{nj-k}{2}$ as modulo n ,

$$\chi_{ijk}(u_{aq\nu}) = \omega^{-2aN((nj-k)+k)^2-2qk^2n} = \omega^{-2qk^2n}.$$

This shows that $\underline{\dim}_{R_{aq\nu}} V_{ijk} = \omega^{-2qk^2n}$.

Let n be an odd integer. In this case, $\chi_{ijk}(E_{ml}) = \delta_{j+k, l} \delta_{\frac{nj-j-k}{2}, m}^{(n)}$ since $n-1, k$ are even, and thus we have

$$\begin{aligned}\chi_{ijk}(u_{aq\nu}) &= \sum_{m=0}^{n-1} \nu^j \omega^{-2aN(2m+j+k)^2-2q(j+k)^2n} \delta_{\frac{nj-j-k}{2}, m}^{(n)} \\ &= \nu^j \omega^{-2aN((nj-j-k)+j+k)^2-2q(j+k)^2n} = \nu^j (-1)^{aj} \omega^{-2q(j+k)^2n}.\end{aligned}$$

This shows that $\underline{\dim}_{R_{aq\nu}} V_{ijk} = \nu^j (-1)^{aj} \omega^{-2q(j+k)^2n}$.

Next we calculate $\underline{\dim}_{R_{aq\nu}} V_{jk}$. Since

$$\begin{aligned}\rho_{jk}(E_{ml}) &= \frac{1}{2nN} \sum_{b=0}^{n-1} \sum_{p=0}^{2N-1} \omega^{-2bN(l+2m)-2lpn} \begin{pmatrix} \omega^{2jN} & 0 \\ 0 & \omega^{-2jN} \end{pmatrix}^b \begin{pmatrix} \omega^{2kn} & 0 \\ 0 & \omega^{2kn} \end{pmatrix}^p \\ &= \delta_{k,l} \begin{pmatrix} \frac{1}{n} \sum_{b=0}^{n-1} \omega^{4bN(\frac{j-k}{2}-m)} & 0 \\ 0 & \frac{1}{n} \sum_{b=0}^{n-1} \omega^{4bN(\frac{-j-k}{2}-m)} \end{pmatrix} \\ &= \delta_{k,l} \begin{pmatrix} \delta_{\frac{j-k}{2}, m}^{(n)} & 0 \\ 0 & \delta_{\frac{-j-k}{2}, m}^{(n)} \end{pmatrix},\end{aligned}$$

we have

$$\rho_{jk}(u_{aq\nu}) = \sum_{m=0}^{n-1} \nu^k \omega^{-2aN(2m+k)^2-2qk^2n} \begin{pmatrix} \delta_{\frac{j-k}{2}, m}^{(n)} & 0 \\ 0 & \delta_{\frac{-j-k}{2}, m}^{(n)} \end{pmatrix}.$$

Thus we have

$$\underline{\dim}_{R_{aq\nu}} V_{jk} = 2\nu^k \omega^{-2aN(2m+k)^2 - 2qk^2n} \delta_{\frac{j-k}{2}, m}^{(n)} = 2\nu^k \omega^{-2aNj^2 - 2qk^2n}.$$

(2) From $\chi_{ijk}(E_l) = \delta_{k,l}$ and $\rho_{1k}(E_l) = \delta_{k,l} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ we have

$$\begin{aligned} \underline{\dim}_{R_d^{(1)}} V_{ijk} &= \underline{\dim}_{R_d^{(2)}} V_{ijk} = \sum_{l=0}^{2N-1} \omega^{-4dl^2} \chi_{ijk}(E_l) = \sum_{l=0}^{2N-1} \omega^{-4dl^2} \delta_{k,l} = \omega^{-4dk^2}, \\ \underline{\dim}_{R_d^{(1)}} V_{1k} &= \underline{\dim}_{R_d^{(2)}} V_{1k} = \sum_{l=0}^{2N-1} \omega^{-4dl^2} \text{Tr} \rho_{1k}(E_l) = \sum_{l=0}^{2N-1} \omega^{-4dl^2} \cdot 2\delta_{k,l} = 2\omega^{-4dk^2}. \end{aligned}$$

□

Combining the results in Proposition 5.16, Proposition 5.17 and Lemma 5.19, we have the following.

Proposition 5.20. *Let $N \geq 1$ be an odd integer, and $n \geq 2$ an integer, and consider the group*

$$G_{Nn} = \langle h, t, w \mid t^2 = h^{2N} = 1, w^n = h^N, tw = w^{-1}t, ht = th, hw = wh \rangle.$$

Let ω be a primitive $4nN$ -th root of unity in a field \mathbf{k} whose characteristic does not divide $2nN$. Then the polynomial invariants of the group Hopf algebra $\mathbf{k}[G_{Nn}]$ are given by the following.

$$P_{\mathbf{k}[G_{Nn}]}^{(1)}(x) = \begin{cases} \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x - \omega^{-8nqs^2})^{4n} (x^2 - \omega^{-4nq(2s+1)^2})^{2n} & (n \text{ is odd}), \\ \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x - \omega^{-8nqs^2})^{8n} & (n \geq 4 \text{ is even}), \\ \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x - \omega^{-16qs^2})^{32} & (n = 2), \end{cases}$$

$$P_{\mathbf{k}[G_{Nn}]}^{(2)}(x) = \begin{cases} \prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n-\epsilon(n)}{2}} \prod_{a=0}^{n-1} \prod_{q=0}^{N-1} (x^2 - \omega^{-4(nq(2s+1)^2 + Na(2t-1)^2)}) \\ \quad \times \prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n-2+\epsilon(n)}{2}} \prod_{a=0}^{n-1} \prod_{q=0}^{N-1} (x - \omega^{-8(nqs^2 + Nat^2)})^2 & (n \geq 3), \\ \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x^4 - \omega^{-16q(2s+1)^2}) (x^2 - \omega^{-8q(2s+1)^2})^2 & (n = 2), \end{cases}$$

where

$$\epsilon(n) = \begin{cases} 0 & n \text{ is even}, \\ 1 & n \text{ is odd}. \end{cases}$$

Proof. First, we consider the case of $n \geq 3$. By Proposition 5.16 any universal R -matrix of $\mathbf{k}[G_{Nn}]$ coincides with exactly one of $R_{aq\nu}$ ($a = 0, 1, \dots, n-1$, $q = 0, 1, \dots, N-1$, $\nu = \pm 1$).

Suppose that $n (\geq 4)$ is even. Then by Lemma 5.19(1), the polynomial invariant $P_{\mathbf{k}[G_{Nn}]}^{(1)}(x)$ is given by

$$P_{\mathbf{k}[G_{Nn}]}^{(1)}(x) = \prod_{i,j=0}^1 \prod_{s=0}^{N-1} P_{\mathbf{k}[G_{Nn}], V_{ij,2s}}(x) = \prod_{i,j=0}^1 \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x - \omega^{-8nqs^2})^{2n} = \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x - \omega^{-8nqs^2})^{8n}.$$

By the same lemma, since $P_{\mathbf{k}[G_{Nn}], V_{jk}}(x)$ is given by $P_{\mathbf{k}[G_{Nn}], V_{jk}}(x) = \prod_{a=0}^{n-1} \prod_{q=0}^{N-1} \prod_{\nu=\pm 1} (x - \nu^k \omega^{-2(nqk^2 + Naj^2)})$ for the simple left $\mathbf{k}[G_{Nn}]$ -module V_{jk} , we have

$$\begin{aligned} P_{\mathbf{k}[G_{Nn}]}^{(2)}(x) &= \left(\prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n}{2}} P_{\mathbf{k}[G_{Nn}], V_{2t-1,2s+1}}(x) \right) \cdot \left(\prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n-2}{2}} P_{\mathbf{k}[G_{Nn}], V_{2t,2s}}(x) \right) \\ &= \prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n}{2}} \prod_{a=0}^{n-1} \prod_{q=0}^{N-1} \prod_{\nu=\pm 1} (x - \nu \omega^{-2(nq(2s+1)^2 + Na(2t-1)^2)}) \\ &\quad \times \prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n-2}{2}} \prod_{a=0}^{n-1} \prod_{q=0}^{N-1} (x - \omega^{-8(nqs^2 + Nat^2)})^2 \\ &= \prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n}{2}} \prod_{a=0}^{n-1} \prod_{q=0}^{N-1} (x^2 - \omega^{-4(nq(2s+1)^2 + Na(2t-1)^2)}) \\ &\quad \times \prod_{s=0}^{N-1} \prod_{t=1}^{\frac{n-2}{2}} \prod_{a=0}^{n-1} \prod_{q=0}^{N-1} (x - \omega^{-8(nqs^2 + Nat^2)})^2. \end{aligned}$$

By a quite similar consideration, we calculate the polynomial invariants of $\mathbf{k}[G_{Nn}]$ in the case where $n (\geq 3)$ is odd.

Next, we consider the case of $n = 2$. Then by Proposition 5.17, any universal R -matrix of $\mathbf{k}[G_{N2}]$ coincides with exactly one of $R_{aq\nu}$ ($a = 0, 1$, $q = 0, 1, \dots, N-1$, $\nu = \pm 1$), $R_d^{(1)}, R_d^{(2)}$ ($d = 0, 1, \dots, 2N-1$). Thus by Lemma 5.19, the polynomial invariant $P_{\mathbf{k}[G_{N2}]}^{(1)}(x)$ is given by

$$\begin{aligned} P_{\mathbf{k}[G_{N2}]}^{(1)}(x) &= \prod_{i,j=0}^1 \prod_{s=0}^{N-1} P_{\mathbf{k}[G_{N2}], V_{ij,2s}}(x) \\ &= \prod_{i,j=0,1} \prod_{s=0}^{N-1} \left(\prod_{q=0}^{N-1} (x - \omega^{-4q(2s)^2})^4 \cdot \prod_{d=0}^{2N-1} (x - \omega^{-4d(2s)^2})^2 \right) \\ &= \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x - \omega^{-16qs^2})^{16} \cdot \prod_{s=0}^{N-1} \prod_{d=0}^{2N-1} (x - \omega^{-16ds^2})^8 \\ &= \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x - \omega^{-16qs^2})^{32}. \end{aligned}$$

Similarly, by Proposition 5.17 and Lemma 5.19, we have

$$\begin{aligned}
P_{\mathbf{k}[G_{N2}]}^{(2)}(x) &= \prod_{s=0}^{N-1} P_{\mathbf{k}[G_{N2}], V_{1,2s+1}}(x) \\
&= \prod_{s=0}^{N-1} \left(\prod_{a=0}^1 \prod_{q=0}^{N-1} \prod_{\nu=\pm 1} (x - \nu \omega^{-2aN-4q(2s+1)^2}) \cdot \prod_{d=0}^{2N-1} (x - \omega^{-4d(2s+1)^2})^2 \right) \\
&= \prod_{s=0}^{N-1} \left(\prod_{a=0}^1 \prod_{q=0}^{N-1} (x^2 - \omega^{-4aN-8q(2s+1)^2}) \cdot \prod_{d=0}^{2N-1} (x - \omega^{-4d(2s+1)^2})^2 \right).
\end{aligned}$$

Here,

$$\begin{aligned}
\prod_{d=0}^{2N-1} (x - \omega^{-4d(2s+1)^2}) &= \prod_{q=0}^{N-1} (x - \omega^{-4q(2s+1)^2}) \cdot \prod_{q=0}^{N-1} (x - \omega^{-4(N+q)(2s+1)^2}) \\
&= \prod_{q=0}^{N-1} (x - \omega^{-4q(2s+1)^2}) \cdot \prod_{q=0}^{N-1} (x + \omega^{-4q(2s+1)^2}) \\
&= \prod_{q=0}^{N-1} (x^2 - \omega^{-8q(2s+1)^2}),
\end{aligned}$$

and whence

$$\begin{aligned}
P_{\mathbf{k}[G_{N2}]}^{(2)}(x) &= \prod_{s=0}^{N-1} \left(\prod_{q=0}^{N-1} (x^2 - \omega^{-4N-8q(2s+1)^2}) \cdot \prod_{q=0}^{N-1} (x^2 - \omega^{-8q(2s+1)^2})^3 \right) \\
&= \prod_{s=0}^{N-1} \prod_{q=0}^{N-1} (x^4 - \omega^{-16q(2s+1)^2}) (x^2 - \omega^{-8q(2s+1)^2})^2.
\end{aligned}$$

□

For an odd integer $N \geq 1$ and an integer $n \geq 2$, we set

$$A_{Nn} = \begin{cases} A_{Nn}^{++} & \text{if } n \text{ is odd,} \\ A_{Nn}^{+-} & \text{if } n \text{ is even.} \end{cases}$$

We see immediately that if n is odd, then $P_{A_{Nn}}^{(d)}(x) = P_{\mathbf{k}[G_{Nn}]}^{(d)}(x)$ for $d = 1, 2$. So, our polynomial invariants do not detect the representation categories of A_{Nn} and $\mathbf{k}[G_{Nn}]$. However, for an even integer n we have:

Corollary 5.21. *Let $N \geq 1$ be an odd integer, and $n \geq 2$ an even integer. Let ω be a primitive $4nN$ -th root of unity in a field \mathbf{k} whose characteristic does not divide $2nN$. Then two Hopf algebras A_{Nn} and $\mathbf{k}[G_{Nn}]$ are not monoidally Morita equivalent.*

Proof. First, let us consider the case of $n \geq 3$, and compare $P_{A_{Nn}}^{(2)}(x)$ and $P_{\mathbf{k}[G_{Nn}]}^{(2)}(x)$. By Corollary 5.12 we see that ω^{-N} is a root of the polynomial $P_{A_{Nn}}^{(2)}(x)$ since n is even. On the other hand, by Proposition 5.20 an arbitrary root of $P_{\mathbf{k}[G_{Nn}]}^{(2)}(x)$ is written in the form ω^{2k} for some integer k . If $P_{A_{Nn}}^{(2)}(x) = P_{\mathbf{k}[G_{Nn}]}^{(2)}(x)$, then $P_{\mathbf{k}[G_{Nn}]}^{(2)}(x)$ has to possess ω^{-N} as a root. Then $\omega^{-N} = \omega^{2k}$ for some k , that is, $N + 2k \equiv 0 \pmod{4nN}$. This leads to a contradiction such that N is even. So, $P_{A_{Nn}}^{(2)}(x) \neq P_{\mathbf{k}[G_{Nn}]}^{(2)}(x)$, and by Theorem 2.6 $A_{Nn}\mathbb{M}$ and $\mathbf{k}[G_{Nn}]\mathbb{M}$ are not equivalent as \mathbf{k} -linear monoidal categories.

Next, let us consider the case of $n = 2$, and compare $P_{A_{N2}}^{(1)}(x)$ and $P_{\mathbf{k}[G_{N2}]}^{(1)}(x)$. By Corollary 5.12 we see that -1 is a root of the polynomial $P_{A_{N2}}^{(1)}(x)$. However, by Proposition 5.20 an arbitrary root of $P_{\mathbf{k}[G_{N2}]}^{(1)}(x)$ is written in the form ω^{16k} for some integer k . By a similar argument above, we see that $-1 = \omega^{4N}$ is not a root of $P_{\mathbf{k}[G_{N2}]}^{(1)}(x)$. Thus $P_{A_{N2}}^{(1)}(x) \neq P_{\mathbf{k}[G_{N2}]}^{(1)}(x)$, and hence by Theorem 2.6 $A_{N2}\mathbb{M}$ and $\mathbf{k}[G_{N2}]\mathbb{M}$ are not equivalent as \mathbf{k} -linear monoidal categories. \square

Example 5.22. For a non-negative integer h , Φ_h denotes the h -th cyclotomic polynomial. Then by using Maple12 software, we see that the polynomial invariants of Hopf algebras $\mathbf{k}[G_{Nn}]$ and A_{Nn} for $N = 1, 3, 5$ and $n = 2, 3, 4$ are given as in the following table.

Hopf algebra A	$P_A^{(1)}(x)$	$P_A^{(2)}(x)$
$\mathbf{k}[G_{12}]$	Φ_1^{32}	$\Phi_4\Phi_2^3\Phi_1^3$
A_{12}	$\Phi_2^{16}\Phi_1^{16}$	$\Phi_8\Phi_2^2\Phi_1^2$
$\mathbf{k}[G_{32}]$	$\Phi_3^{64}\Phi_1^{160}$	$\Phi_{12}^2\Phi_4^5\Phi_6^6\Phi_3^6\Phi_2^{15}\Phi_1^{15}$
A_{32}	$\Phi_6^{32}\Phi_3^{32}\Phi_2^{80}\Phi_1^{80}$	$\Phi_{24}^2\Phi_8^5\Phi_6^4\Phi_3^4\Phi_2^{10}\Phi_1^{10}$
$\mathbf{k}[G_{52}]$	$\Phi_5^{128}\Phi_1^{288}$	$\Phi_{20}^4\Phi_{10}^{12}\Phi_5^{12}\Phi_4^9\Phi_2^{27}\Phi_1^{27}$
A_{52}	$\Phi_{10}^{64}\Phi_5^{64}\Phi_2^{144}\Phi_1^{144}$	$\Phi_{40}^4\Phi_{10}^8\Phi_5^8\Phi_8^9\Phi_2^{18}\Phi_1^{18}$
$\mathbf{k}[G_{13}]$	$\Phi_2^6\Phi_1^{18}$	$\Phi_6\Phi_3^3\Phi_2\Phi_1^3$
A_{13}		
$\mathbf{k}[G_{33}]$	$\Phi_6^{12}\Phi_3^{36}\Phi_2^{30}\Phi_1^{90}$	$\Phi_6^9\Phi_3^{27}\Phi_2^9\Phi_1^{27}$
A_{33}		
$\mathbf{k}[G_{53}]$	$\Phi_{10}^{24}\Phi_5^{72}\Phi_2^{54}\Phi_1^{162}$	$\Phi_{30}^4\Phi_{15}^{12}\Phi_{10}^4\Phi_5^{12}\Phi_6^9\Phi_3^{27}\Phi_2^9\Phi_1^{27}$
A_{53}		
$\mathbf{k}[G_{14}]$	Φ_1^{32}	$\Phi_8^2\Phi_4^2\Phi_2^6\Phi_1^6$
A_{14}		$\Phi_{16}^2\Phi_4^4$
$\mathbf{k}[G_{34}]$	$\Phi_3^{64}\Phi_1^{160}$	$\Phi_{24}^4\Phi_{12}^4\Phi_8^{10}\Phi_6^{12}\Phi_3^{12}\Phi_4^{10}\Phi_2^{30}\Phi_1^{30}$
A_{34}		$\Phi_{48}^4\Phi_{16}^{10}\Phi_{12}^8\Phi_4^{20}$
$\mathbf{k}[G_{54}]$	$\Phi_5^{128}\Phi_1^{288}$	$\Phi_{40}^8\Phi_{20}^8\Phi_{10}^{24}\Phi_5^{24}\Phi_8^{18}\Phi_4^{18}\Phi_2^{54}\Phi_1^{54}$
A_{54}		$\Phi_{80}^8\Phi_{20}^{16}\Phi_{16}^{18}\Phi_4^{36}$

We note that the representation rings of A_{Nn} and $\mathbf{k}[G_{Nn}]$ are isomorphic as rings with $*$ -structure (see Proposition 6.5 for details in the next section). Thus the pair of two Hopf algebras A_{Nn} and $\mathbf{k}[G_{Nn}]$ gives an example of that their representation rings are isomorphic, meanwhile their representation categories are not.

6 Appendix: The representation ring and self-duality of $A_{Nn}^{+\lambda}$

In this appendix, in the case where $N \geq 1$ is odd, by analyzing the algebraic structure of $A_{Nn}^{+\lambda}$ we introduce a “convenient” basis of $A_{Nn}^{+\lambda}$ to compute the braidings $\sigma_{\alpha\beta}$ given in the previous section, and determine the structure of the representation ring of it. As an application, we determine when $A_{Nn}^{+\lambda}$ is self-dual. As one more application, we show that if n is even, then the representation ring of A_{Nn}^{++} is non-commutative. This means that the dual Hopf algebra of $A_{Nn}^{+\lambda}$ has no quasitriangular structure. These results have already shown in [2] in the case of $N = 1$.

Throughout this section we assume that $N \geq 1$ is an odd integer, $n \geq 2$ is an integer, and $\lambda = \pm 1$.

6.1 The algebra structure of $A_{Nn}^{+\lambda}$

First of all, we determine the algebra structure of the Hopf algebra $A_{Nn}^{+\lambda}$. This is done by Masuoka [18] for the case of $N = 1$ (see also [2]).

Proposition 6.1. *Let G be the finite group presented by*

$$G = \langle h, t, w \mid t^2 = h^{2N} = 1, w^n = h^{(n+\frac{\lambda-1}{2})N}, tw = w^{-1}t, ht = th, hw = wh \rangle.$$

Then there is an algebra isomorphism $\varphi : \mathbf{k}[G] \longrightarrow A_{Nn}^{+\lambda}$ such that

$$\varphi(h) = x_{11}^2 - x_{12}^2, \tag{6.1}$$

$$\varphi(t) = x_{12}^N + x_{22}^N, \tag{6.2}$$

$$\varphi(w) = x_{11}^{2N-1}x_{22} - x_{21}^{2N-1}x_{12}. \tag{6.3}$$

Proof. First, we will check the well-definedness of φ . To do this it is sufficient to show that φ preserves the defining relations of G . By definition we have two equations $\varphi(t)^2 = (x_{12}^N + x_{22}^N)^2 = x_{12}^{2N} + x_{22}^{2N} = 1$ and $\varphi(h)^{2N} = (x_{11}^2 - x_{12}^2)^{2N} = x_{11}^{4N} + x_{12}^{4N} = 1$, and since $\varphi(h) = x_{11}^2 - x_{12}^2$ is in the center of $A_{Nn}^{+\lambda}$ by Lemma 5.5, two equations $\varphi(h)\varphi(t) = \varphi(t)\varphi(h)$ and $\varphi(h)\varphi(w) = \varphi(w)\varphi(h)$ are obtained. Now, we set $z = hw$, and define

$$\varphi(z) = x_{11}x_{22} + x_{21}x_{12}.$$

Then we have $\varphi(z) = \varphi(h)\varphi(w)$, and by using Lemma 5.5(5),

$$\begin{aligned} \varphi(z)^n &= (x_{11}x_{22} + x_{21}x_{12})^n = (x_{11}x_{22})^n + (x_{21}x_{12})^n \\ &= x_{11}^{2n} + x_{12}^{2n} = (x_{11}^2 + \lambda x_{12}^2)(x_{11}^2 + x_{12}^2)^{n-1} \\ &= \varphi(h)^{(N+1)n + \frac{\lambda-1}{2}N}. \end{aligned}$$

Therefore, $\varphi(w) = \varphi(h)^{(n+\frac{\lambda-1}{2})N}$. To show the equation $\varphi(t)\varphi(w) = \varphi(w)^{-1}\varphi(t)$, it is sufficient to show that $\varphi(z)\varphi(t)\varphi(z) = \varphi(h)^2\varphi(t)$ since

$$\begin{aligned}\varphi(t)\varphi(w) = \varphi(w)^{-1}\varphi(t) &\iff \varphi(t)\varphi(z) = \varphi(h)\varphi(w)^{-1}\varphi(t) \\ &\iff \varphi(w)\varphi(t)\varphi(z) = \varphi(h)\varphi(t) \\ &\iff \varphi(z)\varphi(t)\varphi(z) = \varphi(h)^2\varphi(t).\end{aligned}$$

The last equation can be derived as follows.

$$\begin{aligned}\varphi(z)\varphi(t)\varphi(z) &= (x_{11}x_{22} + x_{21}x_{12})(x_{12}^N + x_{22}^N)(x_{11}x_{22} + x_{21}x_{12}) \\ &= x_{11}x_{22}^{N+1}x_{11}x_{22} + x_{21}x_{12}^{N+1}x_{21}x_{12} \\ &= x_{11}^2x_{22}^{N+2} + x_{21}^2x_{12}^{N+2} \\ &= (x_{11}^2x_{22}^2 + x_{21}^2x_{12}^2)(x_{22}^N + x_{12}^N) \\ &= (x_{11}^4 + x_{12}^4)(x_{22}^N + x_{12}^N) \\ &= \varphi(h)^2\varphi(t).\end{aligned}$$

Thus there is an algebra map $\varphi : \mathbf{k}[G] \longrightarrow A_{Nn}^{+\lambda}$ satisfying (6.1), (6.2) and (6.3).

Next, we show that φ is surjective. For this, it is enough to show that x_{11} , x_{12} , x_{21} , x_{22} belong to the image of φ . Since N is odd, the equation $x_{22}^2 + x_{12}^2 = x_{11}^2 + x_{12}^2 = \varphi(h)^{N+1}$ holds. Putting $N = 2m + 1$, we have

$$\varphi(t) = (x_{12} + x_{22})(x_{12}^2 + x_{22}^2)^m = (x_{12} + x_{22})\varphi(h)^{m(N+1)},$$

and whence

$$x_{12} + x_{22} = \varphi(th^{-m(N+1)}). \quad (6.4)$$

Since $\varphi(h) = (x_{22} - x_{12})(x_{22} + x_{12}) = (x_{22} - x_{12})\varphi(th^{-m(N+1)})$, we also have

$$x_{22} - x_{12} = \varphi(th^{m(N+1)+1}). \quad (6.5)$$

From the equations (6.4) and (6.5), we see that x_{12}, x_{22} are contained in the image of φ .

Using the equation $x_{11}\varphi(z) = x_{11}(x_{11}x_{22} + x_{21}x_{12}) = x_{11}^2x_{22} = x_{22}^3$, we have $x_{11} = x_{22}^3\varphi(z)^{-1} = x_{22}^3\varphi(z^{-1})$. This shows that x_{11} is in the image of φ . Similarly, using the equation $x_{21}\varphi(z) = x_{21}^2x_{12} = x_{12}^3$ we have $x_{21} = x_{12}^3\varphi(z)^{-1} = x_{12}^3\varphi(z^{-1})$, and whence x_{21} is in the image of φ .

Finally, we show that φ is injective. From $\dim A_{Nn}^{+\lambda} = 4nN$ and the surjectivity of φ , it follows that $4nN = \dim A_{Nn}^{+\lambda} \leq |G|$. On the other hand, since

$$G = \{t^i w^j h^k \mid i = 0, 1, j = 0, 1, \dots, n-1, k = 0, 1, \dots, 2N-1\}$$

as a set, we see that $|G| \leq 4nN$. Therefore, $|G| = 4nN$, and φ is injective. \square

From the above proposition we see that $A_{Nn} \cong \mathbf{k}[G_{Nn}]$ as algebras.

Corollary 6.2. Set $N = 2m + 1$, and consider the following elements in $A_{Nn}^{+\lambda}$:

$$h := x_{11}^2 - x_{12}^2, \quad t := x_{12}^N + x_{22}^N, \quad w := x_{11}^{2N-1}x_{22} - x_{21}^{2N-1}x_{12}.$$

If $ch(\mathbf{k}) \neq 2$, then the following relations hold:

$$(1) \quad t^2 = h^{2N} = 1, \quad w^n = h^{(n+\frac{\lambda-1}{2})N}, \quad tw = w^{-1}t, \quad ht = th, \quad hw = wh.$$

$$(2) \quad x_{22} = \frac{h^{-m(N+1)} + h^{m(N+1)+1}}{2}t, \quad x_{12} = \frac{h^{-m(N+1)} - h^{m(N+1)+1}}{2}t.$$

$$(3) \quad x_{11}^{2N-1} + x_{21}^{2N-1} = wth^{-m(N+1)-1}.$$

$$(4) \quad \begin{cases} x_{11}^N = \frac{h^N+1}{2}wt, \\ x_{21}^N = \frac{h^N-1}{2}wt, \end{cases} \quad \begin{cases} x_{12}^N = -\frac{h^N-1}{2}t, \\ x_{22}^N = \frac{h^N+1}{2}t. \end{cases}$$

$$(5) \quad \begin{cases} x_{11}^{2N-1}x_{22} = \frac{1+h^N}{2}w, \\ x_{21}^{2N-1}x_{12} = \frac{-1+h^N}{2}w, \end{cases} \quad \begin{cases} x_{12}^{2N-1}x_{21} = x_{12}x_{21}^{2N-1} = \frac{h^N-1}{2}w^{-1}, \\ x_{22}^{2N-1}x_{11} = x_{22}x_{11}^{2N-1} = \frac{h^N+1}{2}w^{-1}. \end{cases}$$

In particular,

$$w^{-1} = x_{22}^{2N-1}x_{11} - x_{12}^{2N-1}x_{21}.$$

Proof. The equations in (1) are already derived in the proof of Proposition 6.1. The equations in (2) are obtained by solving the system of linear equations

$$\begin{cases} x_{22} + x_{12} = th^{-m(N+1)}, \\ x_{22} - x_{12} = th^{m(N+1)+1}, \end{cases}$$

which appears in the proof of Proposition 6.1. The equation (3) is obtained by substituting $x_{22} - x_{12} = th^{m(N+1)+1}$ to $w = (x_{11}^{2N-1} + x_{21}^{2N-1})(x_{22} - x_{12})$.

(4) Since $x_{22} - x_{12} = th^{m(N+1)+1}$, and N is odd, we have $x_{22}^N - x_{12}^N = t^N h^{mN(N+1)+N} = th^N$. By solving the system of the equations $x_{22}^N - x_{12}^N = th^N$, $x_{22}^N + x_{12}^N = t$, we get the equations $x_{22}^N = \frac{h^N+1}{2}t$, $x_{12}^N = \frac{1-h^N}{2}t$, and by Parts (2) and (3) we have

$$\begin{aligned} x_{11}^N &= x_{11}^{N+1}(x_{11}^{2N-1} + x_{21}^{2N-1}) \\ &= x_{22}x_{22}^N(x_{11}^{2N-1} + x_{21}^{2N-1}) \\ &= \frac{h^{-m(N+1)} + h^{m(N+1)+1}}{2}t \times \frac{h^N + 1}{2}t \times wth^{-m(N+1)-1} \\ &= wt \frac{h^N + 1}{2}. \end{aligned}$$

We will calculate x_{21}^N . Since $N - 1$ is even, we have

$$\begin{cases} x_{11}^N x_{22}^N = x_{11}^N x_{22}^{N-1} x_{22} = x_{11}^{2N-1} x_{22}, \\ x_{21}^N x_{12}^N = x_{21}^N x_{12}^{N-1} x_{12} = x_{21}^{2N-1} x_{12}. \end{cases}$$

Hence w is expressed as

$$w = x_{11}^N x_{22}^N - x_{21}^N x_{12}^N = (x_{11}^N + x_{21}^N)(x_{22}^N - x_{12}^N) = (x_{11}^N + x_{21}^N)th^N.$$

By postmultiplying th^N to the both sides of the above equation we have $wth^N = x_{11}^N + x_{21}^N$. Thus $x_{21}^N = wth^N - x_{11}^N = \frac{h^N-1}{2}wt$.

(5) From Part (3), we have

$$\begin{aligned} x_{11}^{2N-1}x_{22} + x_{21}^{2N-1}x_{12} &= (x_{11}^{2N-1} + x_{21}^{2N-1})(x_{22} + x_{12}) \\ &= wth^{-m(N+1)-1} \cdot th^{-m(N+1)} = wh^{-2m-1} = wh^N. \end{aligned}$$

By solving the system of the equations $x_{11}^{2N-1}x_{22} + x_{21}^{2N-1}x_{12}wh^N$, $x_{11}^{2N-1}x_{22} - x_{21}^{2N-1}x_{12} = w$, we have $x_{11}^{2N-1}x_{22} = \frac{1+h^N}{2}w$, $x_{21}^{2N-1}x_{12} = \frac{-1+h^N}{2}w$, and whence

$$x_{22}^{2N-1}x_{11} = x_{22}x_{11}^{2N-1} = \frac{h^{-m(N+1)} + h^{m(N+1)+1}}{2}twth^{-m(N+1)-1} = \frac{h^N + 1}{2}w^{-1}.$$

Furthermore, we have $x_{12}^{2N-1}x_{21} = x_{12}x_{21}^{2N-1}$, $x_{22}^{2N-1}x_{11} = x_{22}x_{11}^{2N-1}$, and

$$x_{22}x_{11}^{2N-1} - x_{12}x_{21}^{2N-1} = (x_{22} - x_{12})(x_{11}^{2N-1} + x_{21}^{2N-1}) = th^{m(N+1)+1} \cdot wth^{-m(N+1)-1} = w^{-1}.$$

So, we obtain the desired equation $x_{12}^{2N-1}x_{21} = x_{22}^{2N-1}x_{11} - w^{-1} = \frac{h^N+1}{2}w^{-1} - w^{-1} = \frac{h^N-1}{2}w^{-1}$. \square

Corollary 6.3. *Let G be the finite group presented by*

$$G = \langle h, t, w \mid t^2 = h^{2N} = 1, w^n = h^{(n+\frac{\lambda-1}{2})N}, tw = w^{-1}t, ht = th, hw = wh \rangle.$$

For the group algebra $\mathbf{k}[G]$ over \mathbf{k} of $\text{ch}(\mathbf{k}) \neq 2$, we define algebra maps $\Delta : \mathbf{k}[G] \otimes \mathbf{k}[G] \longrightarrow \mathbf{k}[G]$, $\varepsilon : \mathbf{k}[G] \longrightarrow \mathbf{k}$ and an anti-algebra map $S : \mathbf{k}[G] \longrightarrow \mathbf{k}[G]$ as follows:

$$\begin{aligned} \Delta(h) &= h \otimes h, \quad \Delta(t) = h^N wt \otimes e_1 t + t \otimes e_0 t, \quad \Delta(w) = w \otimes e_0 w + w^{-1} \otimes e_1 w, \\ \varepsilon(h) &= 1, \quad \varepsilon(t) = 1, \quad \varepsilon(w) = 1, \\ S(h) &= h^{-1}, \quad S(t) = (e_0 - e_1 w)t, \quad S(w) = e_0 w^{-1} + e_1 w, \end{aligned}$$

where $e_0 = \frac{1+h^N}{2}$, $e_1 = \frac{1-h^N}{2}$. Then the algebra isomorphism $\varphi : \mathbf{k}[G] \longrightarrow A_{Nn}^{+\lambda}$ defined in Proposition 6.1 is a Hopf algebra isomorphism.

6.2 The representation ring of $A_{Nn}^{+\lambda}$

Via the algebra isomorphism φ given in Proposition 6.1, one can determine the structure of the representation ring of $A_{Nn}^{+\lambda}$.

Let us recall the definition of the representation ring of a semisimple Hopf algebra, which is a natural extension of that of a finite group [20, 21]. Let A be a semisimple Hopf algebra of finite dimension over a field \mathbf{k} . By $\mathfrak{R}(A)$ we denote the set of isomorphism classes of finite-dimensional left A -modules, and for a finite-dimensional left A -module V denote by $[V]$ the isomorphism class of V . Then $\mathfrak{R}(A)$ has a semiring structure induced by

$$[V] + [W] = [V \oplus W], \quad [V][W] = [V \otimes W].$$

Also, $\mathfrak{R}(A)$ has the unit element, which is given by $[\mathbf{k}]$, where the left A -module action of \mathbf{k} is due to the counit ε . Let $\text{Rep}(A)$ denote the Grothendieck group constructed from the enveloping group of $\mathfrak{R}(A)$ as an abelian semigroup. Then the semiring structure of $\mathfrak{R}(A)$ uniquely determines a ring structure of $\text{Rep}(A)$. Furthermore, the ring $\text{Rep}(A)$ has an anti-homomorphism of rings $*$: $\text{Rep}(A) \longrightarrow \text{Rep}(A)$, which induced from the antipode S . Explicitly, this anti-homomorphism $*$ is defined by $[V] \longmapsto [V^*]$ for a finite-dimensional left A -module V . We call the ring $\text{Rep}(A)$ with $*$ the *representation ring* of A . In general, $*$: $\text{Rep}(A) \longrightarrow \text{Rep}(A)$ is not an involution, and the representation ring $\text{Rep}(A)$ is not commutative. However, if the Hopf algebra A possesses a universal R -matrix, then $*$ is an involution, and for two left A -modules V and W an A -linear isomorphism $c_{V,W} : V \otimes W \longrightarrow W \otimes V$ is defined by use of R , and whence we see that $\text{Rep}(A)$ is commutative. We note that $\text{Rep}(A)$ is a free \mathbb{Z} -module with finite rank, and a \mathbb{Z} -basis of $\text{Rep}(A)$ is given by the isomorphism classes of simple left A -modules.

Lemma 6.4. *Let \mathbf{k} be a field whose characteristic dose not divide $2nN$, and suppose that there is a primitive $4nN$ -th root of unity in \mathbf{k} . For integers i, j and an even integer k let χ_{ijk} be the one-dimensional representation of the algebra $A_{Nn} = \mathbf{k}[G_{Nn}]$ given by (5.20), and for integers j, k with $j \equiv k \pmod{2}$ let ρ_{jk} be the two-dimensional representation of the algebra $A_{Nn} = \mathbf{k}[G_{Nn}]$ given by (5.21). We set*

$$\epsilon(n) = \begin{cases} 0 & (n \text{ is even}), \\ 1 & (n \text{ is odd}). \end{cases}$$

Then as representations of the Hopf algebra A_{Nn} the following hold for $i, j, k, i', j', k' \in \mathbb{Z}$.

- (i) $[\rho_{2n+j,k}] = [\rho_{jk}] = [\rho_{-j,k}]$ for $j \equiv k \pmod{2}$, and $[\rho_{n+j,k}] = [\rho_{n-j,k}]$ for $n+j \equiv k \pmod{2}$,
- (ii) $[\rho_{0k}] = [\chi_{00k} \oplus \chi_{10k}]$ for $k \equiv 0 \pmod{2}$, and $[\rho_{nk}] = [\chi_{01,k-\epsilon(n)} \oplus \chi_{11,k-\epsilon(n)}]$ for $k \equiv n \pmod{2}$.
- on representations of tensor products
 - (iii) $[\chi_{ijk} \otimes \chi_{i'j'k'}] = [\chi_{i+i',j+j',k+k'}]$, where k, k' are even,
 - (iv) $[\chi_{ijk} \otimes \rho_{j'k'}] = [\rho_{j'k'} \otimes \chi_{ijk}] = [\rho_{nj+j',k+k'+\epsilon(n)j}]$ for $k \equiv 0, j' \equiv k' \pmod{2}$,
 - (v) $[\rho_{jk} \otimes \rho_{j'k'}] = [\rho_{j+j',k+k'} \oplus \rho_{j-j',k+k'}]$ for $j \equiv k, j' \equiv k' \pmod{2}$.
- on contragredient representations χ_{ijk}^* and ρ_{jk}^*
 - (vi) $[\chi_{ijk}^*] = [\chi_{i,-j,-k}]$ for $k \equiv 0 \pmod{2}$,
 - (vii) $[\rho_{jk}^*] = [\rho_{j,-k}]$ for $j \equiv k \pmod{2}$.

Proof. (i) By definition $[\rho_{2n+j,k}] = [\rho_{j,k}]$ and $[\rho_{-j,k}] = [\rho_{jk}]$ are obtained immediately. By using these equations we have $[\rho_{n+j,k}] = [\rho_{-(n+j),k}] = [\rho_{2n-(n+j),k}] = [\rho_{n-j,k}]$.

(ii) Let $\{e_1, e_2\}$ be the standard basis of $V_{0k} = \mathbf{k} \oplus \mathbf{k}$. Then the subspaces $\mathbf{k}(e_1 + e_2)$ and $\mathbf{k}(e_1 - e_2)$ are ρ_{0k} -invariant, and $\mathbf{k}(e_1 + e_2) = V_{00k}$ and $\mathbf{k}(e_1 - e_2) = V_{10k}$ as submodules of V_{jk} . This implies that $[\rho_{0k}] = [\chi_{00k} \oplus \chi_{10k}]$. Similarly, the subspaces $\mathbf{k}(e_1 + e_2)$ and $\mathbf{k}(e_1 - e_2)$ of V_{nk} are also ρ_{nk} -invariant, and

$$\mathbf{k}(e_1 + e_2) = \begin{cases} V_{01k} & (n \text{ is even}), \\ V_{01,k-1} & (n \text{ is odd}), \end{cases} \quad \text{and} \quad \mathbf{k}(e_1 - e_2) = \begin{cases} V_{11k} & (n \text{ is even}), \\ V_{11,k-1} & (n \text{ is odd}), \end{cases}$$

as submodules of V_{nk} . This proves $[\rho_{nk}] = [\chi_{01,k-\epsilon(n)} \oplus \chi_{11,k-\epsilon(n)}]$.

(iii) It follows from $\chi_{ijk} \otimes \chi_{i'j'k'} = \chi_{i+i', j+j', k+k'}$.

(iv) By using the coproduct Δ given in Corollary 6.3 we see that $(\chi_{ijk} \otimes \rho_{j'k'})(t)$, $(\chi_{ijk} \otimes \rho_{j'k'})(w)$, $(\chi_{ijk} \otimes \rho_{j'k'})(h)$ are represented by the matrices

$$(-1)^{i+k'j} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} \omega^{2(nj+j')N} & 0 \\ 0 & \omega^{-2(nj+j')N} \end{pmatrix}, \quad \omega^{2(k+k'+\epsilon(n)j)n} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

respectively. Let $\{e_1, e_2\}$ be the standard basis of \mathbf{k}^2 . Then by considering the matrix presentation of $\chi_{ijk} \otimes \rho_{j'k'}$ with respect to the basis $\{e_1, (-1)^{i+k'j}e_2\}$, we see that $[\chi_{ijk} \otimes \rho_{j'k'}] = [\rho_{nj+j', k+k'+\epsilon(n)j}]$.

Similarly, we see that if n or j is even, then $(\rho_{j'k'} \otimes \chi_{ijk})(t)$, $(\rho_{j'k'} \otimes \chi_{ijk})(w)$, $(\rho_{j'k'} \otimes \chi_{ijk})(h)$ are represented by the matrices

$$(-1)^i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} \omega^{2(nj+j')N} & 0 \\ 0 & \omega^{-2(nj+j')N} \end{pmatrix}, \quad \omega^{2(k+k'+\epsilon(n)j)n} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

respectively, and if n and j are odd, then they are represented by the matrices

$$(-1)^i \begin{pmatrix} 0 & \omega^{2(nj'+j')N} \\ \omega^{-2(nj'+j')N} & 0 \end{pmatrix}, \quad \begin{pmatrix} \omega^{-2(nj+j')N} & 0 \\ 0 & \omega^{2(nj+j')N} \end{pmatrix}, \quad \omega^{2(k+k'+j)n} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

respectively. So, in the case where n or j is even, by changing basis from $\{e_1, e_2\}$ to $\{e_1, (-1)^i e_2\}$ we see that $[\rho_{j'k'} \otimes \chi_{ijk}] = [\rho_{nj+j', k+k'+\epsilon(n)j}]$, and in the case where n and j are odd, by changing basis from $\{e_1, e_2\}$ to $\{e_2, (-1)^i \omega^{2(nj'+j')N} e_1\}$ we have the same equation $[\rho_{j'k'} \otimes \chi_{ijk}] = [\rho_{nj+j', k+k'+j}]$.

(v) Let $\{e_1, e_2\}$ and $\{e'_1, e'_2\}$ be the bases of V_{jk} and $V_{j'k'}$, such that the matrix representations of ρ_{jk} and $\rho_{j'k'}$ with respect to the bases are given by (5.21), respectively. Then the action of $\rho_{jk} \otimes \rho_{j'k'}$ on $V_{jk} \otimes V_{j'k'}$ is given by

$$\begin{aligned} t \cdot e_a \otimes e'_b &= \begin{cases} e_{3-a} \otimes e'_{3-b} & (\text{if } k' \text{ is even}), \\ \omega^{2(-1)^b(nj+j')N} e_{3-a} \otimes e'_{3-b} & (\text{if } k' \text{ is odd}), \end{cases} \\ w \cdot e_a \otimes e'_b &= \begin{cases} \omega^{2((-1)^{1-a}j+(-1)^{1-b}j')N} e_a \otimes e'_b & (\text{if } k' \text{ is even}), \\ \omega^{2((-1)^a j+(-1)^{1-b}j')N} e_a \otimes e'_b & (\text{if } k' \text{ is odd}), \end{cases} \\ h \cdot e_a \otimes e'_b &= \omega^{2(k+k')n} e_a \otimes e'_b \end{aligned}$$

for $a, b = 1, 2$. Therefore, we see that $[\rho_{jk} \otimes \rho_{j'k'}] = [\rho_{j+j', k+k'} \oplus \rho_{j-j', k+k'}]$ by considering the matrix presentation of $\rho_{jk} \otimes \rho_{j'k'}$ with respect to the basis $\{e_1 \otimes e'_1, e_2 \otimes e'_2, e_1 \otimes e'_2, e_2 \otimes e'_1\}$ or $\{e_2 \otimes e'_1, \omega^{2(jn-j)N} e_1 \otimes e'_2, e_2 \otimes e'_2, \omega^{2(jn+j)N} e_1 \otimes e'_1\}$ according to the case whether k' is even or odd.

(vi) Since $\chi_{ijk}^*(t) = (-1)^i$, $\chi_{ijk}^*(w) = (-1)^{-j}$, $\chi_{ijk}^*(h) = \omega^{-2(k+\epsilon(n)j)n}$, we have $\chi_{ijk}^* = \chi_{i, -j, -k}$.

(vii) Let $\{e_1, e_2\}$ be the standard basis of $V_{jk} = \mathbf{k} \oplus \mathbf{k}$. Then with respect to the dual basis $\{e_1^*, e_2^*\}$ of $\{e_1, e_2\}$, the contragredient representation ρ_{jk}^* is represented as follows: $\rho_{jk}^*(h) = \begin{pmatrix} \omega^{-2kn} & 0 \\ 0 & \omega^{-2kn} \end{pmatrix}$, and

if k is even, then $\rho_{jk}^*(t) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\rho_{jk}^*(w) = \begin{pmatrix} \omega^{-2jN} & 0 \\ 0 & \omega^{2jN} \end{pmatrix}$, and

if k is odd, then $\rho_{jk}^*(t) = \begin{pmatrix} 0 & -\omega^{-2jN} \\ -\omega^{2jN} & 0 \end{pmatrix}$, $\rho_{jk}^*(w) = \begin{pmatrix} \omega^{2jN} & 0 \\ 0 & \omega^{-2jN} \end{pmatrix}$. Thus in the case where k is even, by considering the matrix presentation of ρ_{jk}^* with respect to the basis $\{e_2^*, e_1^*\}$, we see that $[\rho_{jk}^*] = [\rho_{j, -k}]$. In the case where k is odd, by considering the matrix presentation of ρ_{jk}^* with respect to the basis $\{e_1^*, -\omega^{2jN} e_2^*\}$, we have the same result $[\rho_{jk}^*] = [\rho_{j, -k}]$. \square

From the above lemma, we see that the representation ring of A_{Nn} is described as in the following proposition. In the case of $N = 1$, this result has already proved by [18, Proposition 3.9].

Proposition 6.5. *Let \mathbf{k} be a field whose characteristic dose not divide $2nN$, and suppose that there is a primitive $4nN$ -th root of unity in \mathbf{k} .*

(1) *If n is even, then the representation rings of A_{Nn} and $\mathbf{k}[G_{Nn}]$ are isomorphic as rings with $*$ -structure, and both of them are isomorphic to the commutative ring generated by $a, b, c, x_1, \dots, x_{n-1}$ subject to the commutativity relations and the following relations:*

$$a^2 = b^2 = c^N = 1, \quad (6.6)$$

$$ax_i = x_i \quad (i = 1, 2, \dots, n-1), \quad (6.7)$$

$$bx_i = x_{n-i} \quad (i = 1, 2, \dots, n-1), \quad (6.8)$$

$$x_i x_j = c^{\frac{1-(-1)^{ij}}{2}} (x_{|i-j|} + x_{i+j}) \quad (i, j = 1, 2, \dots, n-1), \quad (6.9)$$

where indices of x in R.H.S. of (6.9) are treated under the rules

$$x_0 = 1 + a, \quad x_n = b(1 + a), \quad x_{n+i} = x_{n-i} \quad (i = 1, 2, \dots, n-1).$$

The $*$ -structure is given by

$$a^* = a, \quad b^* = b, \quad c^* = c^{-1}, \quad x_i^* = c^{\frac{(-1)^i - 1}{2}} x_i \quad (i = 1, \dots, n-1).$$

(2) If n is odd, then the representation rings of A_{Nn} and $\mathbf{k}[G_{Nn}]$ are isomorphic as rings with $*$ -structure, and both of them are isomorphic to the commutative ring generated by $a, b, x_1, \dots, x_{n-1}$ subject to the commutativity relations and the following relations:

$$a^2 = b^{2N} = 1, \quad (6.10)$$

$$ax_i = x_i \quad (i = 1, \dots, n-1), \quad (6.11)$$

$$bx_i = x_{n-i} \quad (i = 2, 4, \dots, n-1), \quad (6.12)$$

$$x_i x_j = b^{1-(-1)^{ij}} (x_{|i-j|} + x_{i+j}) \quad (i, j = 1, \dots, n-1) \quad (6.13)$$

where indices of x in R.H.S. of (6.13) are treated under the rules

$$x_0 = 1 + a, \quad x_n = b(1 + a), \quad x_{n+i} = x_{n-i} \quad (i = 1, 2, \dots, n-1).$$

The $*$ -structure is given by

$$a^* = a, \quad b^* = b^{-1}, \quad x_i^* = b^{(-1)^i - 1} x_i \quad (i = 1, \dots, n-1).$$

Proof. Since the same results in Lemma 6.4 hold for the group Hopf algebra $\mathbf{k}[G_{Nn}]$, it is sufficient to prove that the representation ring of A_{Nn} is isomorphic to the commutative ring \mathcal{R} which is presented by the given generators and relations described in the proposition. By Proposition 6.1 we may assume that $A_{Nn} = \mathbf{k}[G_{Nn}]$ as algebras.

(1) We will prove that the representation ring $\text{Rep}(A_{Nn})$ is the commutative ring generated by $a = [\chi_{100}]$, $b = [\chi_{010}]$, $c = [\chi_{002}]$, $x_i = [\rho_{i\epsilon(i)}]$ ($i = 1, \dots, n-1$) with relations (6.6), (6.8), (6.7) and (6.9), where χ_{ijk} and ρ_{jk} are the one-dimensional and two-dimensional representations of the algebra $A_{Nn} = \mathbf{k}[G_{Nn}]$ given by (5.20) and (5.21), respectively, and $\epsilon(i)$ is equal to 0 or 1 according to whether i is even or odd, respectively.

Since $[\chi_{000}] = [\varepsilon] = 1$, by Lemma 6.4(iii) it follows that $a^2 = b^2 = c^N = 1$. By Parts (i) and (iv) of Lemma 6.4, we have

$$ax_i = [\chi_{100}][\rho_{i\epsilon(i)}] = [\rho_{i,\epsilon(i)}] = x_i,$$

and

$$bx_i = [\chi_{010}][\rho_{i\epsilon(i)}] = [\rho_{n+i,\epsilon(i)}] = [\rho_{n-i,\epsilon(i)}] = x_{n-i}.$$

Furthermore, for integers $i, j \in \mathbb{Z}$, by Parts (iv) and (v) of Lemma 6.4 we have

$$\begin{aligned} x_i x_j &= [\rho_{i-j,\epsilon(i)+\epsilon(j)}] + [\rho_{i+j,\epsilon(i)+\epsilon(j)}] \\ &= \begin{cases} x_{i-j} + x_{i+j} = x_{|i-j|} + x_{i+j} & (i \text{ or } j \text{ is even}), \\ [\rho_{i-j,2}] + [\rho_{i+j,2}] = [\chi_{002}][\rho_{i-j,0}] + [\rho_{i+j,0}] & (i \text{ and } j \text{ are odd}), \end{cases} \\ &= c^{\frac{1-(-1)^{ij}}{2}} (x_{|i-j|} + x_{i+j}). \end{aligned}$$

By Lemma 6.4(ii) we have

$$x_0 = [\chi_{000}] + [\chi_{100}] = 1 + a, \quad x_n = [\chi_{010}] + [\chi_{110}] = [\chi_{010}] + [\chi_{010}][\chi_{100}] = b(1 + a),$$

and by Lemma 6.4(i) we have

$$x_{n+i} = [\rho_{n+i, \epsilon(n+i)}] = [\rho_{n-i, \epsilon(n+i)}] = [\rho_{n-i, \epsilon(n-i)}] = x_{n-i}.$$

From the results argued so far, we see that there is a ring homomorphism $f : \mathcal{R} \longrightarrow \text{Rep}(A_{Nn})$ such that

$$f(a) = [\chi_{100}], \quad f(b) = [\chi_{010}], \quad f(c) = [\chi_{002}], \quad f(x_i) = [\rho_{i\epsilon(i)}] \quad (i = 1, 2, \dots, n-1).$$

To show that f is bijective, let us construct the inverse map of f . Let $g : \text{Rep}(A_{Nn}) \longrightarrow \mathcal{R}$ be the \mathbb{Z} -linear map defined by

$$\begin{aligned} g([\chi_{ijk}]) &= a^i b^j c^{\frac{k}{2}} \quad (i, j = 0, 1, \quad k = 0, 2, \dots, 2N-2), \\ g([\rho_{jk}]) &= c^{\frac{k-\epsilon(j)}{2}} x_j \quad (k = 0, 1, \dots, 2N-1, \quad j = 1, 2, \dots, n-1, \quad j \equiv k \pmod{2}). \end{aligned}$$

Then it is easily shown that g is the inverse map of f , and this concludes that $f : \mathcal{R} \longrightarrow \text{Rep}(A_{Nn})$ is a ring isomorphism.

The $*$ -structure in $\text{Rep}(A_{Nn})$ is determined as follows. By Lemma 6.4(vi) we see immediately that $a^* = a$, $b^* = b$, $c^* = [\chi_{00, -2}] = [\chi_{002}]^{N-1} = c^{N-1} = c^{-1}$. By Lemma 6.4(vii) if i is even, then $x_i^* = [\rho_{i0}]^* = [\rho_{i0}] = x_i$, and if i is odd, then $x_i^* = [\rho_{i1}]^* = [\rho_{i, -1}] = [\rho_{i, 2N-1}] = [\chi_{00, 2N-2} \otimes \rho_{i1}] = [\chi_{002}]^{N-1} [\rho_{i1}] = c^{-1} x_i$. Therefore, we obtain $x_i^* = c^{\frac{(-1)^i - 1}{2}} x_i$ for $i = 1, 2, \dots, n-1$.

(2) In the same manner as above it can be verified that there is a ring isomorphism $f : \mathcal{R} \longrightarrow \text{Rep}(A_{Nn})$ such that $f(a) = [\chi_{100}]$, $f(b) = [\chi_{010}]$, $f(x_i) = [\rho_{i\epsilon(i)}]$ ($i = 1, \dots, n-1$) preserving $*$ -structures. Here, what we should take account is the following fact. If we set $b = [\chi_{010}]$, then $[\chi_{002}] = b^2$, and since n is odd, it follows from Parts (i) and (iv) of Lemma 6.4 that

$$bx_i = [\chi_{010}][\rho_{i\epsilon(i)}] = [\rho_{n+i, 1+\epsilon(i)}] = [\rho_{n-i, 1+\epsilon(i)}] = \begin{cases} [\chi_{002} \otimes \rho_{n-i, 0}] = b^2 x_{n-i} & (i \text{ is odd}), \\ [\chi_{000} \otimes \rho_{n-i, 1}] = x_{n-i} & (i \text{ is even}). \end{cases}$$

This is equivalent to $bx_i = x_{n-i}$ for all even integers i . □

Remark 6.6. By Proposition 6.1 in the case where $(\lambda, n) = (+, \text{even})$ or $(\lambda, n) = (-, \text{odd})$, as an algebra $A_{Nn}^{+\lambda}$ is isomorphic to the group algebra $\mathbf{k}[G'_{Nn}]$, where

$$G'_{Nn} = \langle h, t, w \mid t^2 = h^{2N} = 1, w^n = 1, tw = w^{-1}t, ht = th, hw = wh \rangle.$$

As a similar manner of the proofs of Lemma 6.4 and Proposition 6.5, one can determine the structure of $\text{Rep}(A_{Nn}^{++})$ in the case where n is even, and the structure of $\text{Rep}(A_{Nn}^{+-})$ in the case where n is odd. As a result, we see that in the case where n is even the representation ring $\text{Rep}(A_{Nn}^{++})$ is not commutative (see Lemma 6.11 in the next subsection 6.3), whereas the representation ring $\text{Rep}(\mathbf{k}[G'_{Nn}])$ is commutative since $\mathbf{k}[G'_{Nn}]$ is cocommutative. Therefore, two representation rings of A_{Nn}^{++} and $\mathbf{k}[G'_{Nn}]$ are not isomorphic. On the contrary, in the case where n is odd, we see that $\text{Rep}(A_{Nn}^{+-}) \otimes_{\mathbb{Z}} \mathbf{k}$ and $\text{Rep}(\mathbf{k}[G'_{Nn}]) \otimes_{\mathbb{Z}} \mathbf{k}$ are isomorphic as algebras with $*$ -structure over \mathbf{k} .

6.3 Self-duality of $A_{Nn}^{+\lambda}$

Based on Corollary 6.3, we identify $A_{Nn}^{+\lambda}$ with $\mathbf{k}[G]$ such as

$$\begin{aligned} h &= x_{11}^2 - x_{12}^2, \\ t &= x_{12}^N + x_{22}^N = x_{11}^{N-1}x_{22} + x_{12}^N, \\ w &= x_{11}^{2N-1}x_{22} - x_{21}^{2N-1}x_{12} = x_{11}^{2N-1}\chi_{22} - x_{12}^{2N-2}\chi_{21}^2. \end{aligned}$$

Then

$$w^{-1} = x_{22}x_{11}^{2N-1} - x_{12}x_{21}^{2N-1} = x_{11}^{2N-2}\chi_{22}^2 - x_{12}^{2N-1}\chi_{21}.$$

Let us determine the values of $\sigma_{\alpha\beta}$ on the elements of the basis $\{h^i w^k t^p \mid 0 \leq i \leq 2N-1, 0 \leq k \leq n-1, p=0,1\}$ of $A_{Nn}^{+\lambda}$.

Lemma 6.7. *Suppose that $\alpha, \beta \in \mathbf{k}$ satisfy $(\alpha\beta)^N = 1$ and $(\alpha\beta^{-1})^n = \lambda$, and consider the braiding $\sigma_{\alpha\beta}$ of $A_{Nn}^{+\lambda}$ defined in Theorem 5.8. We set $\xi := \alpha\beta$ and $\eta := \alpha\beta^{-1}$. Then for $i, j, k, l \geq 0$ the following equations hold:*

$$\sigma_{\alpha\beta}(h^i w^k, h^j w^l) = \xi^{2ij} \eta^{-2kl}, \quad (6.14)$$

$$\sigma_{\alpha\beta}(h^i w^k, h^j w^l t) = (-1)^{i+k} \xi^{2ij} \eta^{-k(2l-1)}, \quad (6.15)$$

$$\sigma_{\alpha\beta}(h^i w^k t, h^j w^l) = (-1)^{j+l} \xi^{2ij} \eta^{(2k-1)l}, \quad (6.16)$$

$$\sigma_{\alpha\beta}(h^i w^k t, h^j w^l t) = (-1)^{i+j+k+l} \xi^{2ij+\frac{N^2-1}{2}} \eta^{2kl-k-l} \alpha. \quad (6.17)$$

Proof. First, we show $\sigma_{\alpha\beta}(h^i w^k, h^j w^l) = \xi^{2ij} \eta^{-2kl}$. In the case of $k=0$ the above equation is written as $\sigma_{\alpha\beta}(h^i, h^j w^l) = (\alpha\beta)^{2ij}$. This can be proved by induction on l as follows. By use of the equation $h^j = x_{11}^{2j} + (-1)^j x_{12}^{2j}$ ($j \geq 0$), we see that

$$\begin{aligned} \sigma_{\alpha\beta}(h^i, h^j) &= \sigma_{\alpha\beta}(x_{11}^{2i}, x_{11}^{2j}) + (-1)^j \sigma_{\alpha\beta}(x_{11}^{2i}, x_{12}^{2j}) \\ &\quad + (-1)^i \sigma_{\alpha\beta}(x_{12}^{2i}, x_{11}^{2j}) + (-1)^{i+j} \sigma_{\alpha\beta}(x_{12}^{2i}, x_{12}^{2j}) \\ &= \sigma_{\alpha\beta}(x_{11}^{2i}, x_{11}^{2j}) = (\alpha\beta)^{2ij}. \end{aligned}$$

Suppose that $\sigma_{\alpha\beta}(h^i, h^j w^l) = (\alpha\beta)^{2ij}$ for some $l \geq 0$. Since

$$\begin{aligned} \sigma_{\alpha\beta}(h^i, w) &= \sigma_{\alpha\beta}(x_{11}^{2i}, x_{11}^{2N-1}\chi_{22}) - \sigma_{\alpha\beta}(x_{11}^{2i}, x_{12}^{2N-2}\chi_{21}^2) \\ &\quad + (-1)^i \sigma_{\alpha\beta}(x_{12}^{2i}, x_{11}^{2N-1}\chi_{22}) - (-1)^i \sigma_{\alpha\beta}(x_{12}^{2i}, x_{12}^{2N-2}\chi_{21}^2) \\ &= \sigma_{\alpha\beta}(x_{11}^{2i}, x_{11}^{2N-1}\chi_{22}) = (\alpha\beta)^{2iN} = 1, \end{aligned}$$

it follows that

$$\sigma_{\alpha\beta}(h^i, h^j w^{l+1}) = \sigma_{\alpha\beta}(h^i, w) \sigma_{\alpha\beta}(h^i, h^j w^l) = \sigma_{\alpha\beta}(h^i, h^j w^l) = (\alpha\beta)^{2ij}.$$

So, it is true for $l+1$.

Now, let $k \geq 1$, and suppose that $\sigma_{\alpha\beta}(h^i w^k, h^j w^l) = (\alpha\beta)^{2ij}(\alpha^{-1}\beta)^{2kl}$ for all $l \geq 0$. Then we have

$$\begin{aligned}\sigma_{\alpha\beta}(h^i w^{k+1}, h^j w^l) &= \sigma_{\alpha\beta}(h^i w^k, h^j w^l) \sigma_{\alpha\beta}(w, h^j e_0 w^l) + \sigma_{\alpha\beta}(h^i w^k, h^j w^{l-1}) \sigma_{\alpha\beta}(w, h^j e_1 w^l) \\ &= \sigma_{\alpha\beta}(h^i w^k, h^j w^l) \sigma_{\alpha\beta}(w, h^j w^l) \\ &= (\alpha\beta)^{2ij}(\alpha^{-1}\beta)^{2kl} \times (\alpha^{-1}\beta)^{2l} \\ &= (\alpha\beta)^{2ij}(\alpha^{-1}\beta)^{2(k+1)l}.\end{aligned}$$

Thus it is true for $k+1$, and the equation (6.14) is proved by induction on k .

Second, we show (6.15). By use of (6.14) we have

$$\begin{aligned}\sigma_{\alpha\beta}(h^i w^k, h^j w^l t) &= \sigma_{\alpha\beta}(h^i w^k, t) \sigma_{\alpha\beta}(h^i e_0 w^k, h^j w^l) + \sigma_{\alpha\beta}(h^i w^{k-1}, t) \sigma_{\alpha\beta}(h^i e_1 w^k, h^j w^l) \\ &= \sigma_{\alpha\beta}(h^i w^k, t) (\alpha\beta)^{2ij} (\alpha^{-1}\beta)^{2kl}.\end{aligned}$$

By induction on k we can show that $\sigma_{\alpha\beta}(h^i w^k, t) = (-\alpha\beta^{-1})^k (-1)^i$, and thus the equation (6.15) holds.

As a similar manner we can show that $\sigma_{\alpha\beta}(h^i w^k, h^j w^{-l}) = (\alpha\beta)^{2ij} (\alpha\beta^{-1})^{2kl}$, $\sigma_{\alpha\beta}(t, h^j w^l) = (-\alpha^{-1}\beta)^l (-1)^j$, and the equation (6.16) holds.

Finally, we show that (6.17). For $a, b \in \{0, 1\}$ we have

$$\begin{aligned}\sigma_{\alpha\beta}(e_a t, h^j e_b w^l) &= \frac{1}{4} \left(\sigma_{\alpha\beta}(t, h^j w^l) + (-1)^b \sigma_{\alpha\beta}(t, h^{j+N} w^l) \right. \\ &\quad \left. + (-1)^a \sigma_{\alpha\beta}(h^N t, h^j w^l) + (-1)^{a+b} \sigma_{\alpha\beta}(h^N t, h^{j+N} w^l) \right) \\ &= \frac{1 + (-1)^{b+1} + (-1)^a + (-1)^{a+b+1}}{4} (-1)^j (-\alpha^{-1}\beta)^l \\ &= \begin{cases} (-1)^j (-\alpha^{-1}\beta)^l & \text{if } a \text{ is even, and } b \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Since $\sigma_{\alpha\beta}(t, t) = \sigma_{\alpha\beta}(x_{11}^{N-1} \chi_{22} + x_{12}^N, x_{11}^{N-1} \chi_{22} + x_{12}^N) = \sigma_{\alpha\beta}(x_{12}^N, x_{12}^N) = (\alpha\beta)^{\frac{N^2-1}{2}} \alpha$, we have

$$\begin{aligned}\sigma_{\alpha\beta}(t, h^j e_a w^l t) &= \sigma_{\alpha\beta}(h^N w t, t) \sigma_{\alpha\beta}(e_1 t, h^j e_a w^l) + \sigma_{\alpha\beta}(t, t) \sigma_{\alpha\beta}(e_0 t, h^j e_a w^l) \\ &= \begin{cases} 0 & (a = 0), \\ (\alpha\beta)^{\frac{N^2-1}{2}} \alpha (-1)^j (-\alpha^{-1}\beta)^l & (a = 1). \end{cases}\end{aligned}$$

So, by using the equation $\sigma_{\alpha\beta}(h^i w^k, h^j w^{-l} t) = (-1)^{i+k} (\alpha\beta)^{2ij} (\alpha\beta^{-1})^{k(2l+1)}$, we have

$$\begin{aligned}\sigma_{\alpha\beta}(h^i w^k t, h^j w^l t) &= \sigma_{\alpha\beta}(h^i w^k, h^j w^l t) \sigma_{\alpha\beta}(t, h^j e_0 w^l t) \\ &\quad + \sigma_{\alpha\beta}(h^i w^k, h^{j+N} w^{-l+1} t) \sigma_{\alpha\beta}(t, h^j e_1 w^l t) \\ &= \sigma_{\alpha\beta}(h^i w^k, h^{j+N} w^{-l+1} t) \sigma_{\alpha\beta}(t, t) (-1)^j (-\alpha^{-1}\beta)^l \\ &= (-1)^{i+k} (\alpha\beta)^{2i(j+N)} (\alpha\beta^{-1})^{k(2(l-1)+1)} \cdot (\alpha\beta)^{\frac{N^2-1}{2}} \alpha (-1)^j (-\alpha^{-1}\beta)^l \\ &= (-1)^{i+j+k+l} (\alpha\beta)^{2ij+\frac{N^2-1}{2}} (\alpha\beta^{-1})^{2kl-k-l} \alpha.\end{aligned}$$

□

From here to the end of the paper, we suppose that \mathbf{k} is a field whose characteristic does not divide $2nN$, and it contains a primitive $4nN$ -th root of unity.

Theorem 6.8. *Let α, β be elements in \mathbf{k} satisfying $(\alpha\beta)^N = 1$ and $(\alpha\beta^{-1})^n = \lambda$. Suppose that $\lambda = -1$ or $(\lambda, n) = (1, \text{odd})$. Then the braiding $\sigma_{\alpha\beta}$ of $A_{Nn}^{+\lambda}$ is non-degenerate if and only if*

- (i) $\alpha\beta$ is a primitive N -th root of unity, and
- (ii) $\alpha\beta^{-1}$ is a primitive n -th root of λ .

Proof. To show “if” part, we show the contraposition.

Suppose that $\alpha\beta$ is not a primitive N -th root of unity. Then $N \geq 3$ is required since if $N = 1$, then $\alpha\beta = (\alpha\beta)^N = 1$. Let ξ be a primitive N -th root of unity. Then $\alpha\beta$ is represented by $\alpha\beta = \xi^m$ for some divisor m ($\neq 1$) of N . Hence by setting $m' := N/m$ ($< N$), we have

$$\begin{aligned}\sigma_{\alpha\beta}(h^{2m'}, h^j w^l) &= (\alpha\beta)^{4m'j} = \xi^{4mm'j} = \xi^{4Nj} = 1 = \sigma_{\alpha\beta}(1, h^j w^l), \\ \sigma_{\alpha\beta}(h^{2m'}, h^j w^l t) &= (-1)^{2m'} (\alpha\beta)^{4m'j} = 1 = \sigma_{\alpha\beta}(1, h^j w^l t).\end{aligned}$$

Thus $\sigma_{\alpha\beta}(1 - h^{2m'}, a) = 0$ for all $a \in A_{Nn}^{+\lambda}$. Since $1 < 2m' < 2N$, we see that $1 - h^{2m'} \neq 0$. Therefore, $\sigma_{\alpha\beta}$ degenerates as a bilinear form on $A_{Nn}^{+\lambda}$.

Next, suppose that $\alpha\beta^{-1}$ is not a primitive n -th root of λ . Then there is an $r \in \mathbb{N}$ such that $1 \leq r < n$ and $(\alpha\beta^{-1})^r = \lambda$. So, $(\alpha\beta^{-1})^{n-r} = 1$. By Lemma 6.7 we have

$$\begin{aligned}\sigma_{\alpha\beta}(w^{n-r}, h^j w^l) &= (\alpha\beta^{-1})^{-2(n-r)l} = 1, \\ \sigma_{\alpha\beta}(w^{n-r}, h^j w^l t) &= (-1)^{n-r} (\alpha\beta^{-1})^{-(n-r)(2l-1)} = (-1)^{n-r}.\end{aligned}$$

If $n - r$ is even, then

$$\begin{aligned}\sigma_{\alpha\beta}(w^{n-r}, h^j w^l) &= 1 = \sigma_{\alpha\beta}(1, h^j w^l), \\ \sigma_{\alpha\beta}(w^{n-r}, h^j w^l t) &= 1 = \sigma_{\alpha\beta}(1, h^j w^l t).\end{aligned}$$

Thus $\sigma_{\alpha\beta}(1 - w^{n-r}, a) = 0$ for all $a \in A_{Nn}^{+\lambda}$. It follows from $0 < n - r \leq n - 1$ that $1 - w^{n-r} \neq 0$, and hence $\sigma_{\alpha\beta}$ degenerates.

If $n - r$ is odd, then

$$\begin{aligned}\sigma_{\alpha\beta}(w^{n-r}, h^j w^l) &= 1 = \sigma_{\alpha\beta}(h^N, h^j w^l), \\ \sigma_{\alpha\beta}(w^{n-r}, h^j w^l t) &= -1 = \sigma_{\alpha\beta}(h^N, h^j w^l t).\end{aligned}$$

Thus $\sigma_{\alpha\beta}(h^N - w^{n-r}, a) = 0$ for all $a \in A_{Nn}^{+\lambda}$. Since $h^N - w^{n-r} \neq 0$, the braiding $\sigma_{\alpha\beta}$ also degenerates as a bilinear form.

We will show “only if” part. Let us consider the linear map $F : A_{Nn}^{+\lambda} \longrightarrow (A_{Nn}^{+\lambda})^*$ defined by

$$F(a) = \sum_{j=0}^{2N-1} \sum_{l=0}^{n-1} \sigma_{\alpha\beta}(a, h^j w^l) (h^j w^l)^* + \sum_{j=0}^{2N-1} \sum_{l=0}^{n-1} \sigma_{\alpha\beta}(a, h^j w^l t) (h^j w^l t)^* \quad (a \in A_{Nn}^{+\lambda}).$$

Here, $\{ (h^j w^l t^p)^* \mid 0 \leq j \leq 2N-1, 0 \leq l \leq n, p=0,1 \}$ stands for the dual basis of the basis $\{ h^j w^l t^p \mid 0 \leq j \leq 2N-1, 0 \leq l \leq n, p=0,1 \}$ of $A_{Nn}^{+\lambda}$. Setting $\xi = \alpha\beta$, $\eta = \alpha\beta^{-1}$, we have

$$F(h^i w^k) = \sum_{j=0}^{2N-1} \sum_{l=0}^{n-1} \xi^{2ij} \eta^{-2kl} ((h^j w^l)^* + (-1)^{i+k} \eta^k (h^j w^l t)^*),$$

$$F(h^i w^k t) = \sum_{j=0}^{2N-1} \sum_{l=0}^{n-1} (-1)^{j+l} \xi^{2ij} \eta^{2kl-l} ((h^j w^l)^* + (-1)^{i+k} \xi^{\frac{N^2-1}{2}} \eta^{-k} \alpha (h^j w^l t)^*).$$

In what follows, let ξ be a primitive N -th root of unity, and η is a primitive n -th root of λ . We consider the case of $N \geq 3$. Since N is odd, the following claims hold for $j \in \mathbb{Z}$:

- $\xi^{2j} = 1 \iff j \equiv 0 \pmod{N}$,
- $\xi^{2j} \neq -1$.

Therefore, for $j, j' \in \mathbb{Z}$, we have

$$\sum_{i=0}^{2N-1} \xi^{2i(j-j')} = \begin{cases} 2N & \text{if } j \equiv j' \pmod{N}, \\ 0 & \text{otherwise,} \end{cases} \quad \sum_{i=0}^{2N-1} (-1)^i \xi^{2i(j-j')} = 0.$$

Thus we have

$$\sum_{i=0}^{2N-1} \xi^{-2ij'} F(h^i w^k) = 2N \sum_{l=0}^{n-1} \eta^{-2kl} ((h^{j'} w^l)^* + (h^{j'+N} w^l)^*),$$

$$\sum_{i=0}^{2N-1} \xi^{-2ij'} F(h^i w^k t) = 2N \sum_{l=0}^{n-1} (-1)^{j'+l} \eta^{2kl-l} ((h^{j'} w^l)^* - (h^{j'+N} w^l)^*).$$

Since $\eta^{2(l-l')} = 1$ if and only if $l - l' \equiv 0 \pmod{n}$ under the condition $\lambda = -1$ or $(\lambda, n) = (1, \text{odd})$, it follows that for $l' \in \mathbb{Z}$

$$\sum_{k=0}^{n-1} \eta^{2k(l-l')} = \begin{cases} 0 & \text{otherwise,} \\ n & \text{if } l \equiv l' \pmod{n}. \end{cases} \quad (6.18)$$

This implies that

$$\sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} \eta^{2kl'} \xi^{-2ij'} F(h^i w^k) = 2nN ((h^{j'} w^{l'})^* + (h^{j'+N} w^{l'})^*),$$

$$\sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} \eta^{-2kl'} \xi^{-2ij'} F(h^i w^k t) = 2nN (-1)^{j'+l'} \eta^{-l'} ((h^{j'} w^{l'})^* - (h^{j'+N} w^{l'})^*).$$

From these equations, we have

$$(h^{j'} w^{l'})^* = \frac{1}{4nN} \left(\sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} \eta^{2kl'} \xi^{-2ij'} F(h^i w^k) + (-1)^{j'+l'} \eta^{l'} \sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} \eta^{-2kl'} \xi^{-2ij'} F(h^i w^k t) \right),$$

$$(h^{j'+N} w^{l'})^* = \frac{1}{4nN} \left(\sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} \eta^{2kl'} \xi^{-2ij'} F(h^i w^k) - (-1)^{j'+l'} \eta^{l'} \sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} \eta^{-2kl'} \xi^{-2ij'} F(h^i w^k t) \right).$$

As a similar manner, we have

$$\begin{aligned} \sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} (-1)^{i+k} \eta^{2kl'-k} \xi^{-2ij'} F(h^i w^k) &= 2nN((h^{j'} w^{l'} t)^* + (h^{j'+N} w^{l'} t)^*), \\ \sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} (-1)^{i+k} \eta^{-2kl'+k} \xi^{-2ij'} F(h^i w^k t) &= 2nN(-1)^{j'+l'} \xi^{\frac{N^2-1}{2}} \eta^{-l'} \alpha((h^{j'} w^{l'} t)^* - (h^{j'+N} w^{l'} t)^*), \end{aligned}$$

and

$$\begin{aligned} (h^{j'} w^{l'} t)^* &= \frac{1}{4nN} \left(\sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} (-1)^{i+k} \eta^{2kl'-k} \xi^{-2ij'} F(h^i w^k) \right. \\ &\quad \left. + (-1)^{j'+l'} \xi^{-\frac{N^2-1}{2}} \eta^{l'} \alpha^{-1} \sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} (-1)^{i+k} \eta^{-2kl'+k} \xi^{-2ij'} F(h^i w^k t) \right), \\ (h^{j'+N} w^{l'} t)^* &= \frac{1}{4nN} \left(\sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} (-1)^{i+k} \eta^{2kl'-k} \xi^{-2ij'} F(h^i w^k) \right. \\ &\quad \left. - (-1)^{j'+l'} \xi^{-\frac{N^2-1}{2}} \eta^{l'} \alpha^{-1} \sum_{i=0}^{2N-1} \sum_{k=0}^{n-1} (-1)^{i+k} \eta^{-2kl'+k} \xi^{-2ij'} F(h^i w^k t) \right). \end{aligned}$$

Thus F is surjective, and whence F is an isomorphism. This implies that $\sigma_{\alpha\beta}$ is non-degenerate.

We consider the case of $N = 1$. Then $\xi = 1$, and

$$\begin{aligned} F(h^i w^k) &= \sum_{j=0}^1 \sum_{l=0}^{n-1} \eta^{-2kl} ((h^j w^l)^* + (-1)^{i+k} \eta^k (h^j w^l t)^*), \\ F(h^i w^k t) &= \sum_{j=0}^1 \sum_{l=0}^{n-1} (-1)^{j+l} \eta^{2kl-l} ((h^j w^l)^* + (-1)^{i+k} \eta^{-k} \alpha (h^j w^l t)^*). \end{aligned}$$

As a similar manner as above, we see that $(w^{l'})^*, (hw^{l'})^*, (w^{l'} t)^*, (hw^{l'} t)^*$ can be represented by linear combinations of $\{F(h^i w^k), F(h^i w^k t)\}$, and hence $\sigma_{\alpha\beta}$ is non-degenerate. \square

Corollary 6.9. *Suppose that $\lambda = -1$, or $(\lambda, n) = (1, \text{odd})$. Then the Hopf algebra $A_{Nn}^{+\lambda}$ is self-dual.*

Proof. In general, for a finite-dimensional Hopf algebra A , any braiding $\sigma : A \otimes A \longrightarrow \mathbf{k}$ gives rise to the Hopf pairing $\langle \cdot, \cdot \rangle : A^{\text{cop}} \otimes A \longrightarrow \mathbf{k}$ defined by $\langle x, y \rangle = \sigma(x, y)$ for $x, y \in A$, and this pairing induces a Hopf algebra map $F : A \longrightarrow (A^{\text{cop}})^*$ defined by $(F(a))(b) = \sigma(a, b)$ for $a, b \in A$. Applying this fact to the Hopf algebra $A_{Nn}^{+\lambda}$ and the braiding $\sigma_{\alpha\beta}$, we have a Hopf algebra map $F : A_{Nn}^{+\lambda} \longrightarrow ((A_{Nn}^{+\lambda})^{\text{cop}})^*$. Furthermore, an algebra isomorphism $\phi : A_{Nn}^{+\lambda} \longrightarrow A_{Nn}^{+\lambda}$ can be defined by $\phi(x_{ij}) = x_{ji}$ ($i, j = 1, 2$), and we see that it becomes a Hopf algebra isomorphism from $A_{Nn}^{+\lambda}$ to $(A_{Nn}^{+\lambda})^{\text{cop}}$ [30]. So, if $\sigma_{\alpha\beta}$ is non-degenerate, then the composition ${}^t\phi \circ F : A_{Nn}^{+\lambda} \longrightarrow (A_{Nn}^{+\lambda})^*$ gives a Hopf algebra isomorphism.

To complete the proof, by Theorem 6.8, it suffices to show that there are α, β such that $\alpha\beta$ is a primitive N -th root of unity, and $\alpha\beta^{-1}$ is a primitive n -th root of λ . Let $\omega \in \mathbf{k}$ be a primitive $4nN$ -th root of unity. In the case of $\lambda = -1$, we take $\alpha = \omega^{N+2n}$, $\beta = \omega^{2n-N}$. Then $\alpha\beta^{-1} = \omega^{2N}$ is a primitive n -th root of -1 , and $\alpha\beta = \omega^{4n}$ is a primitive N -th root of unity. In the case where $\lambda = 1$ and n is odd, we take $\alpha = \omega^{2N+2n}$, $\beta = \omega^{2n-2N}$. Then $\alpha\beta^{-1} = \omega^{4N}$ and $\alpha\beta = \omega^{4n}$ are primitive n -th and primitive N -th roots of unity, respectively. \square

To show that A_{Nn}^{++} is not self-dual for any even integer n , we compare the groups of group-like elements of A_{Nn}^{++} and $(A_{Nn}^{++})^*$. The structure of $G(A_{Nn}^{\nu\lambda})$ for all $N \geq 1, n \geq 2$ and $\lambda, \nu = \pm 1$ has already determined by S. Suzuki [30]. In the case where N is odd, and $\nu = +$ the group $G(A_{Nn}^{\nu\lambda})$ is given as follows.

Lemma 6.10 (S.Suzuki).

$$G(A_{Nn}^{+\lambda}) \cong \begin{cases} C_2 \times C_{2N} & (n \text{ is even, or } (n, \lambda) = (\text{odd}, 1)), \\ C_{4N} & (n \text{ is odd, and } \lambda = -1). \end{cases}$$

On the contrary, we have:

Lemma 6.11. *The structure of $G((A_{Nn}^{++})^*)$ is given as follows.*

$$\begin{aligned} G((A_{Nn}^{++})^*) &\cong \begin{cases} SA_{8N} & (n \text{ is even}), \\ C_2 \times C_{2N} & (n \text{ is odd}), \end{cases} \\ G((A_{Nn}^{+-})^*) &\cong \begin{cases} C_2 \times C_2 \times C_N & (n \text{ is even}), \\ C_{4N} & (n \text{ is odd}), \end{cases} \end{aligned}$$

where SA_{8N} is the finite group of order $8N$ defined by

$$SA_{8N} = \langle b, c \mid b^2 = c^{4N} = 1, cb = bc^{2N+1} \rangle.$$

Proof. Let ω be a primitive $4nN$ -th root of unity.

(1) If n is even, then for fixed integers i, j, k there is an algebra map $\chi_{ijk} : A_{Nn}^{++} \rightarrow \mathbf{k}$ such that $\chi_{ijk}(t) = (-1)^i$, $\chi_{ijk}(w) = (-1)^j$, $\chi_{ijk}(h) = \omega^{2nk}$. Since any algebra map $A_{Nn}^{++} \rightarrow \mathbf{k}$ coincides with some χ_{ijk} , we have $G((A_{Nn}^{++})^*) = \{ \chi_{ijk} \mid i, j = 0, 1, k = 0, 1, \dots, 2N-1 \}$. Furthermore, since the product of $G((A_{Nn}^{++})^*)$ is given by

$$\chi_{ijk}\chi_{i'j'k'} = \chi_{i+i'+(j+k)k', j+j', k+k'} \quad (i, i', j, j', k, k' \in \mathbb{Z}),$$

$a := \chi_{100}$, $b := \chi_{010}$, $c := \chi_{001}$ satisfy the equations $a^2 = b^2 = 1$, $c^{2N} = a$, $cb = bc^{2N+1}$. Thus we have $G((A_{Nn}^{++})^*) = \langle b, c \mid b^2 = c^{4N} = 1, cb = bc^{2N+1} \rangle = SA_{8N}$.

If n is odd, then for fixed integers i, k there is an algebra map $\chi_{ik} : A_{Nn}^{++} \rightarrow \mathbf{k}$ such that $\chi_{ik}(t) = (-1)^i$, $\chi_{ik}(w) = (-1)^k$, $\chi_{ik}(h) = \omega^{2nk}$. Since any algebra map $A_{Nn}^{++} \rightarrow \mathbf{k}$ coincides with some χ_{ik} , we have $G((A_{Nn}^{++})^*) = \{ \chi_{ik} \mid i = 0, 1, k = 0, 1, \dots, 2N-1 \}$. Furthermore, since the product of $G((A_{Nn}^{++})^*)$ is given by

$$\chi_{ik}\chi_{i'k'} = \chi_{i+i', k+k'} \quad (i, i', k, k' \in \mathbb{Z}),$$

we see that $G((A_{Nn}^{++})^*) \cong C_2 \times C_{2N}$.

(2) If n is even, then as the same manner with the proof of Part (1) we see that $G((A_{Nn}^{+-})^*) = \{ \chi_{ijk} \mid i, j = 0, 1, k = 0, 2, \dots, 2N-2 \}$, where $\chi_{ijk} : A_{Nn}^{+-} \longrightarrow \mathbf{k}$ is the algebra map such that $\chi_{ijk}(t) = (-1)^i$, $\chi_{ijk}(w) = (-1)^j$, $\chi_{ijk}(h) = \omega^{2nk}$. The product of $G((A_{Nn}^{+-})^*)$ is given by $\chi_{ijk}\chi_{i'j'k'} = \chi_{i+i', j+j', k+k'}$ for all $i, i', j, j', k, k' \in \mathbb{Z}$. Thus the group $G((A_{Nn}^{+-})^*)$ is commutative. Since $a := \chi_{100}$, $b := \chi_{010}$, $c := \chi_{002}$ satisfy the equations $a^2 = b^2 = 1$, $c^N = 1$, we see that $G((A_{Nn}^{+-})^*) = C_2 \times C_2 \times C_N$.

If n is odd, then, $G((A_{Nn}^{+-})^*) = \{ \chi_{ik} \mid i = 0, 1, k = 0, 2, \dots, 2N-2 \}$, where $\chi_{ik} : A_{Nn}^{+-} \longrightarrow \mathbf{k}$ is the algebra map such that $\chi_{ik}(t) = (-1)^i$, $\chi_{ik}(w) = 1$, $\chi_{ik}(h) = \omega^{2nk}$. Since the product of $G((A_{Nn}^{+-})^*)$ is given by $\chi_{ik}\chi_{i'k'} = \chi_{i+i'+kk', k+k'}$ for all $i, i', k, k' \in \mathbb{Z}$, we see that the group $G((A_{Nn}^{+-})^*)$ is commutative. Furthermore, $a := \chi_{10}$ and $b := \chi_{01}$ satisfy the equations $a^2 = 1$, $b^{2N} = a$, and hence $G((A_{Nn}^{+-})^*) = C_{4N}$. \square

If a semisimple Hopf algebra A possesses a quasitriangular structure, the representation ring needs to be commutative. In the case where $N \geq 1$ is odd, and n is even, by Lemma 6.11 the representation ring of the dual Hopf algebra $(A_{Nn}^{++})^*$ are not commutative, and therefore there is no quasitriangular structure of $(A_{Nn}^{++})^*$.

By Lemma 6.10 and Lemma 6.11 we have:

Proposition 6.12. *If n is even, then the Hopf algebra A_{Nn}^{++} is not self-dual.*

Proof. The group $G(A_{Nn}^{++}) \cong C_2 \times C_{2N}$ is commutative by Lemma 6.10, meanwhile $G((A_{Nn}^{++})^*) \cong SA_{8N}$ is not by Lemma 6.11. This implies that $G(A_{Nn}^{++}) \not\cong G((A_{Nn}^{++})^*)$, and $A_{Nn}^{++} \not\cong (A_{Nn}^{++})^*$. \square

Corollary 6.13. *If n is even, then all braidings of A_{Nn}^{++} degenerate.*

Proof. Assume that there is a non-degenerate braiding of A_{Nn}^{++} . Then there is a Hopf algebra isomorphism $F : A_{Nn}^{++} \longrightarrow ((A_{Nn}^{++})^{\text{cop}})^*$. Let us consider the Hopf algebra isomorphism $\phi : A_{Nn}^{++} \longrightarrow (A_{Nn}^{++})^{\text{cop}}$ defined by $\phi(x_{ij}) = x_{ji}$ ($i, j = 1, 2$). Then the composition $\iota\phi \circ F : A_{Nn}^{++} \longrightarrow (A_{Nn}^{++})^*$ is also a Hopf algebra isomorphism. This contradicts Proposition 6.12. \square

Acknowledgements

The author would like to thank Professor Akira Masuoka and Professor Ikuo Satake for helpful advice and discussions. Thanks are also due to Professor Juan Cuadra for his suggestions to improve my preliminary version of the proof of Lemma 5.1. This research is partially supported by Grant-in-Aid for Scientific Research (No. 19540025), JSPS.

References

- [1] E. Abe, Hopf Algebras, Cambridge Univ. Press, Cambridge, 1980 (original Japanese version published by Iwanami Shoten, Tokyo, 1977).
- [2] C. Călinescu, S. Dăscălescu, A. Masuoka, C. Menini, Quantum lines over non-cocommutative cosemisimple Hopf algebras, *J. Algebra* 273 (2004) 753–779.
- [3] Y. Doi, Braided bialgebras and quadratic bialgebras, *Comm. Algebra* 21 (1993) 1731–1749.
- [4] Y. Doi, M. Takeuchi, Quaternion algebras and Hopf crossed products, *Comm. Algebra* 23 (1995) 3291–3325.
- [5] V. G. Drinfel'd, Quantum groups, In: *Proceedings of the International Congress of Mathematics*, Berkeley, CA., 1987, pp. 798–820.
- [6] P. Etingof, S. Gelaki, On finite-dimensional semisimple and cosemisimple Hopf algebras in positive characteristic, *Int. Math. Research Notices* no. 16 (1998) 851–864.
- [7] P. Etingof, S. Gelaki, On the exponent of finite-dimensional Hopf algebras, *Math. Research Lett.* 6 (1999) 131–140.
- [8] A. Joyal, R. Street, Braided tensor categories, *Adv. Math.* 102 (1993) 20–78.
- [9] G. I. Kac, V. G. Paljutkin, Finite ring groups, in: *Transactions of the Moscow Mathematical Society for the year 1966*, AMS, 1967, 251–294 (original Russian paper: *Trudy Moscov. Math. Ob.* 15 (1966) 224–261).
- [10] R.G. Larson, Characters of Hopf algebras, *J. Algebra* 17 (1971) 352–368.
- [11] R.G. Larson, D.E. Radford, Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple, *J. Algebra* 117 (1988) 267–289.
- [12] R.G. Larson, D.E. Radford, Semisimple cosemisimple Hopf algebras, *Amer. J. Math.* 110 (1988) 187–195.
- [13] R.G. Larson, D.E. Radford, Semisimple Hopf algebras, *J. Algebra* 171 (1995) 5–35.
- [14] S. MacLane, *Categories for the working mathematician*, G.T.M. 5, Springer-Verlag, New York, 1971.
- [15] S. Majid, Representation-theoretic rank and double Hopf algebras, *Comm. Algebra* 18 (1990) 3705–3712.
- [16] A. Masuoka, Cleft extensions for a Hopf algebra generated by a nearly primitive element, *Comm. Algebra* 22 (1994) 4537–4559.
- [17] A. Masuoka, Semisimple Hopf algebras of dimension 6, 8, *Israel J. Math.* 92 (1995) 361–373.

- [18] A. Masuoka, Cocycle deformations and Galois objects for some cosemisimple Hopf algebras of finite dimension, *Contemp. Math.* 267 (2000) 195–214.
- [19] S. Montgomery, Hopf algebras and their action on rings, C.B.M.S. 82, American Mathematical Society, 1993.
- [20] W. D. Nichols, M. B. Richmond, The Grothendieck group of a Hopf algebra, *J. Pure and Appl. Algebra* 106 (1996) 297–306.
- [21] D. Nikshych, K_0 -rings and twisting of finite dimensional semisimple Hopf algebras, *Comm. Algebra* 26 (1998) 321–342; Erratum: *Comm. Algebra* 26 (1998) 1347.
- [22] D. E. Radford, The group of automorphisms of a semisimple Hopf algebra over a field of characteristic 0, *Amer. J. Math.* 112 (1990) 331–357.
- [23] D. E. Radford, On the quasitriangular structures of a semisimple Hopf algebra, *J. Algebra* 141 (1991) 354–358.
- [24] D. E. Radford, On the antipode of a quasitriangular Hopf algebra, *J. Algebra* 151 (1992) 1–11.
- [25] D. E. Radford, Minimal quasitriangular Hopf algebras, *J. Algebra* 157 (1993) 285–315.
- [26] P. Schauenburg, On coquasitriangular Hopf algebras and the quantum Yang-Baxter equation, *Algebra Berichte* 67, Verlag Reinhard Fischer, 1992.
- [27] P. Schauenburg, Hopf bigalois extensions, *Comm. Algebra* 24 (1996) 3797–3825.
- [28] P. Schauenburg, Bi-Galois objects over the Taft algebras, *Israel J. Math.* 115 (2000) 101–123.
- [29] P. Schauenburg, Hopf-Galois and Bi-Galois extensions, In: *Galois theory, Hopf algebras, and semiabelian categories* (Fields Inst. Comm. 43), edited by G. Janelidze, B. Pareigis and W. Tholen, A.M.S., Providence, RI, 2004, pp. 469–515.
- [30] S. Suzuki, A family of braided cosemisimple Hopf algebras of finite dimension, *Tsukuba J. Math.* 22 (1998) 1–29.
- [31] M. E. Sweedler, *Hopf algebras*, Benjamin, New York, 1969.
- [32] D. Tambara, S. Yamagami, Tensor categories with fusion rules of self-duality for finite abelian groups, *J. of Algebra* 209 (1998) 692–707.
- [33] M. Wakui, On the universal R-matrices of the dihedral groups (in Japanese), *Sūrikaiseikikenkyūsho Kōkyūroku* 1057 (1998) 41–53.
- [34] W. C. Waterhouse, *Introduction to affine group schemes*, G.T.M. 66, Springer-Verlag, 1979.

- [35] W. C. Waterhouse, Automorphism group schemes of semisimple cosemisimple Hopf algebras, *Amer. J. Math.* 115 (1993) 691–698.